

DOT/FAA/AR-97/80

Office of Aviation Research
Washington, DC 20591

**Threat Image Projection User Guides
for Federal Security Managers,
Security Company Managers, and
Checkpoint Security Supervisors
Using EG&G Astrophysics Linescan
X-Ray Machines**



PB98-126204

J. L. Fobes, Ph.D.
Eric C. Neiderman, Ph.D.
Brenda A. Klock
J. Michael Barrientos

Aviation Security Human Factors
Program, AAR-510
William J. Hughes Technical Center
Atlantic City International Airport, NJ 08405

October 1997
Final Report

This document is available to the U.S. public
through the National Technical Information
Service, Springfield, Virginia 22161



U.S. Department of Transportation
William J. Hughes Technical Center

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

1. Report No. DOT/FAA/AR-97/80		2. Government Accession No.		3. Recipient's Catalog No.	
4. Title and Subtitle Threat Image Projection User Guides for Federal Security Managers, Security Company Managers, and Checkpoint Security Supervisors Using EG&G Astrophysics Linescan X-Ray Machine				5. Report Date	
				6. Performing Organization Code AAR-510	
7. Author(s) J. L. Fobes, Ph.D., Eric C. Neiderman, Ph.D., Brenda A. Klock, and J. Michael Barrientos				8. Performing Organization Report No. DOT/FAA/AR-97/80	
9. Performing Organization Name and Address Federal Aviation Administration William J. Hughes Technical Center Atlantic City International Airport, NJ 08405				10. Work Unit No. (TRAIS)	
				11. Contract or Grant No. DTFA03-94-C-00012	
12. Sponsoring Agency Name and Address US Department of Transportation Federal Aviation Administration Associate Administrator of Civil Aviation Security 800 Independence Ave., S.W. Washington, DC 20591				13. Type of Report and Period Covered Covered Final Report	
				14. Sponsoring Agency Code ACS-1	
15. Supplementary Notes Prepared by Michael D. Snyder, NYMA, Inc.					
16. Abstract This document provides step-by-step instructions for Federal Security Managers (FSMs), Security Company Managers (SCMs), and Checkpoint Security Supervisors (CSSs) operating the Threat Image Projection (TIP) system. This system was developed by EG&G Astrophysics for its Linescan X-ray machines. This document is comprised of two independent user guides. The first explains functions available to FSMs and SCMs. These functions include user administration (i.e., adding, modifying, and deleting users), management of the TIP Image Library and presentation schedule, and downloading monthly reports. The second guide explains functions available to CSSs. These functions include logging in and out of the system and viewing reports. In addition to explaining how to view a report, it explains what each report contains.					
17. Key Words Threat Image Projection Federal Security Manager Checkpoint Security Supervisor Security Company Manager				18. Distribution Statement This document is available to the public through the National Technical Information Service, Springfield, Virginia, 22161	
19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified		21. No. of Pages 100	22. Price	

Preface

These user guides are step-by-step instructions for TIP management functions. The key FAA personnel supporting these guides are J. L. Fobes, Ph.D., Eric C. Neiderman, Ph.D., Brenda A. Klock, and J. M. Barrientos with the Aviation Security Research and Development Division, Human Factors Program (AAR-510).

Table of Contents

	Page
Preface.....	iii
Executive Summary	ix
User Guide I	
Introduction.....	1
What is in this guide?.....	1
What functions are covered?.....	1
Security Access Levels	2
How is access to TIP functions and reports controlled?	2
Who will be able to do what?	2
TIP System User Administration	3
What topics will be covered in this section?.....	3
What can I change?.....	3
What are my options when I want to locate a TIP user?.....	4
How do I scroll through the user list?.....	6
How do I find a TIP user by name or ID number?	8
How do I add a new user?.....	10
How do I change TIP user information?.....	12
How do I set or change a user's password?	14
How do I set or change a user's security access level?.....	16
How do I delete a user?.....	18
How do I change an active user to inactive status?.....	20
Management of the TIP Image Library.....	22
What is the TIP Image Library?.....	23
What topics will be covered in this section?.....	23
What new terms will I need to know for this section?.....	23
How do I locate a specific threat in the TIP Image Library?	24
How do I set TIP to include specific threats?	26
How do I set TIP to include all threat images of a specific category and subcategory?.....	28
How do I set TIP to exclude a specific threat image?.....	30
How do I set TIP to exclude all threat images of a specific category and subcategory?	32
How do I view a threat image on the screen?	34
How do I add a new threat into the Image Library?	36
How do I download a threat from the Image Library?	38
How do I upload a threat from a disk?.....	40
How do I delete a threat from the TIP Image Library?.....	42
How do I add a new subcategory?	44

Table of Contents (Cont.)

	Page
Management of the Threat Image Presentation Schedule.....	47
What is the threat image presentation schedule?	47
What topics will be covered in this section?.....	47
How does the schedule work?.....	47
How do I set threat presentation frequency ratios?.....	48
How do I set the percentages of threats to be presented?	50
Downloading Monthly Data Reports	52
What is involved?	52
How do I download the Screener Log Report?.....	52
How do I download the Individual Screener Performance Report?	54
How do I download the Screener Comparisons Report?	56
How do I download the Threat Image Projection Details Report?.....	58
Where do I send the monthly data disks?	60
 User Guide II	
Threat Image Projection System: Overview for EG&G X-ray Machines	1
What is Threat Image Projection (TIP)?.....	1
What does TIP do?.....	1
How does TIP work?	1
What is the purpose of this training?	1
What will this guide tell me?	1
Log In.....	2
Who can log in?	2
How do I log in?	2
Security Access Levels	4
How is access to TIP functions and reports controlled?	4
Who will be able to do what?	4
Report Overviews	5
What reports are available?.....	5
How does TIP generate these reports?.....	5
Screener Log Report: Overview and Generation	6
What is a Screener Log Report?	6
What does each column heading mean?	6
How do I view a Screener Log Report?.....	8

Table of Contents (Cont)

	Page
Individual Screener Performance Summary Comparisons Report: Overview and Generation	10
What is a Screener Performance Report?	10
What does each column heading mean?	10
How do I view an Individual Screener Performance Report?	12
Screener Comparisons Report: Overview and Generation	14
What is a Screener Comparisons Report?.....	14
What does each column heading mean?	14
How do I get a Screener Comparisons Report?	16
Threat Image Projection Details Report: Overview and Generation	18
What is a Threat Image Projection Details Report?.....	18
What does each column heading mean?	18
How do I get a Threat Image Projections Details Report?	20
Log Out	22
How do I log out?	22

Executive Summary

The Threat Image Projection (TIP) system is a software addition to the X-ray machine. It randomly inserts fictional threats (guns, knives, bombs, etc.) onto X-ray images of actual passenger bags. In addition to integrating images of threats and actual baggage, TIP will also insert images of fictitious bags containing threats.

This document provides step-by-step instructions for Federal Security Managers (FSMs), Security Company Managers (SCMs), and Checkpoint Security Supervisors (CSSs) operating the EG&G Astrophysics' TIP system. Because some TIP functions were not intended for all users, two independent users' guides were developed, one for the FSMs and SCMs and the other for CSSs.

This document is comprised of both users' guides. The guide intended for FSMs and SCMs to use is provided first. It describes functions only available to them such as user administration (i.e., adding, modifying, and deleting users), management of the TIP Image Library and presentation schedule, and downloading monthly reports.

The guide intended for CSSs is provided second. This guide explains functions such as logging in and out of the system and viewing reports. In addition to explaining how to view a report, the guide explains what each report contains.

**EG&G Astrophysics
Threat Image Projection
Federal Security Managers'
and
Security Company Managers' Guide**



User Guide I

Table of Contents

	Page
Introduction.....	1
What is in this guide?.....	1
What functions are covered?.....	1
Security Access Levels	2
How is access to TIP functions and reports controlled?	2
Who will be able to do what?	2
TIP System User Administration	3
What topics will be covered in this section?.....	3
What can I change?.....	3
What are my options when I want to locate a TIP user?.....	4
How do I scroll through the user list?.....	6
How do I find a TIP user by name or ID number?	8
How do I add a new user?.....	10
How do I change TIP user information?.....	12
How do I set or change a user's password?	14
How do I set or change a user's security access level?.....	16
How do I delete a user?.....	18
How do I change an active user to inactive status?.....	20
Management of the TIP Image Library.....	22
What is the TIP Image Library?.....	23
What topics will be covered in this section?.....	23
What new terms will I need to know for this section?.....	23
How do I locate a specific threat in the TIP Image Library?	24
How do I set TIP to include specific threats?	26
How do I set TIP to include all threat images of a specific category and subcategory?.....	28
How do I set TIP to exclude a specific threat image?.....	30
How do I set TIP to exclude all threat images of a specific category and subcategory?	32
How do I view a threat image on the screen?	34
How do I add a new threat into the Image Library?	36
How do I download a threat from the Image Library?	38
How do I upload a threat from a disk?.....	40
How do I delete a threat from the TIP Image Library?.....	42
How do I add a new subcategory?	44
Management of the Threat Image Presentation Schedule.....	47
What is the threat image presentation schedule?	47
What topics will be covered in this section?.....	47
How does the schedule work?.....	47
How do I set threat presentation frequency ratios?.....	48
How do I set the percentages of threats to be presented?	50

Table of Contents (Cont.)

	Page
Downloading Monthly Data Reports.....	52
What is involved?	52
How do I download the Screener Log Report?.....	52
How do I download the Individual Screener Performance Report?	54
How do I download the Screener Comparisons Report?	56
How do I download the Threat Image Projection Details Report?	58
Where do I send the monthly data disks?	60

Introduction

This Threat Image Projection (TIP) Guide is provided for use by managers. Security Access Level 1 or 2 is required to access the functions covered below and effect changes in the TIP image presentation and scheduling module.

What is in this guide?

This guide contains step-by-step instructions for TIP management functions.

What functions are covered?

1. TIP system user administration
2. Management of the TIP Image Library
3. Management of the threat image presentation schedule
4. Downloading monthly data reports

Security Access Levels

How is access to TIP functions and reports controlled?

There are multiple security access levels depending on the user's needs. This guide pertains only to the levels for Federal Security Managers (FSMs) and Security Company Managers. The user ID number and password tell the computer the access level of each user.

Who will be able to do what?

Table 1 shows who may access different functions and reports generated by the TIP system.

All users are able to perform the functions within their cell and below (e.g., FSMs and the FAA can also download and upload data, maintain operators, view TIP reports, and log in and log out).

Table 1. TIP User Levels and Functions

USER	CAPABILITIES
Federal Security Manager FAA Personnel	Sets scheduling Sets presentation ratios Selects threat categories Manages TIP Image Library
Station Manager Security Company Manager Ground Security Coordinator	User administration functions Download reports
Checkpoint Security Supervisor	View TIP reports
Screener in Charge Screener	Log in Log out

Note: Screeners will only be able to log in and log out of baggage screening equipment. They will not have access to TIP reports or data.

TIP System User Administration

What topics will be covered in this section?

1. Finding a specific TIP user
2. Adding a new TIP user
3. Changing TIP user information
4. Changing a TIP user's password
5. Changing a TIP user's security access level
6. Deleting a TIP user

What can I change?

If you have the security access level of an FSM or Security Company Manager, you can change all user information except performance data. If you have the security access level of a Station Manager, you can change all user information for your level and below, however, you cannot delete a user. (Note: Station Managers cannot view user information for any higher-level individuals.)

What are my options when I want to locate a TIP user?

(See Figure 1)

There are two methods to find a specific TIP user.

1. Scroll through the user list. The four buttons that you use to scroll through the user list are mentioned below. The User Administration screen automatically starts with a display of the first user list entry.
 - a. Top - Brings up the first entry on the TIP user list.
 - b. Previous - Brings up the previous entry on the TIP user list.
 - c. Next - Brings up the next entry on the TIP user list.
 - d. Bottom - Brings up the last entry on the TIP user list.
2. Find an individual by name or by ID number. The button that will assist you in finding a specific user by name or ID number is listed below.
 - a. Find - Brings up another screen that allows you to choose to view the list of users by name or ID number.

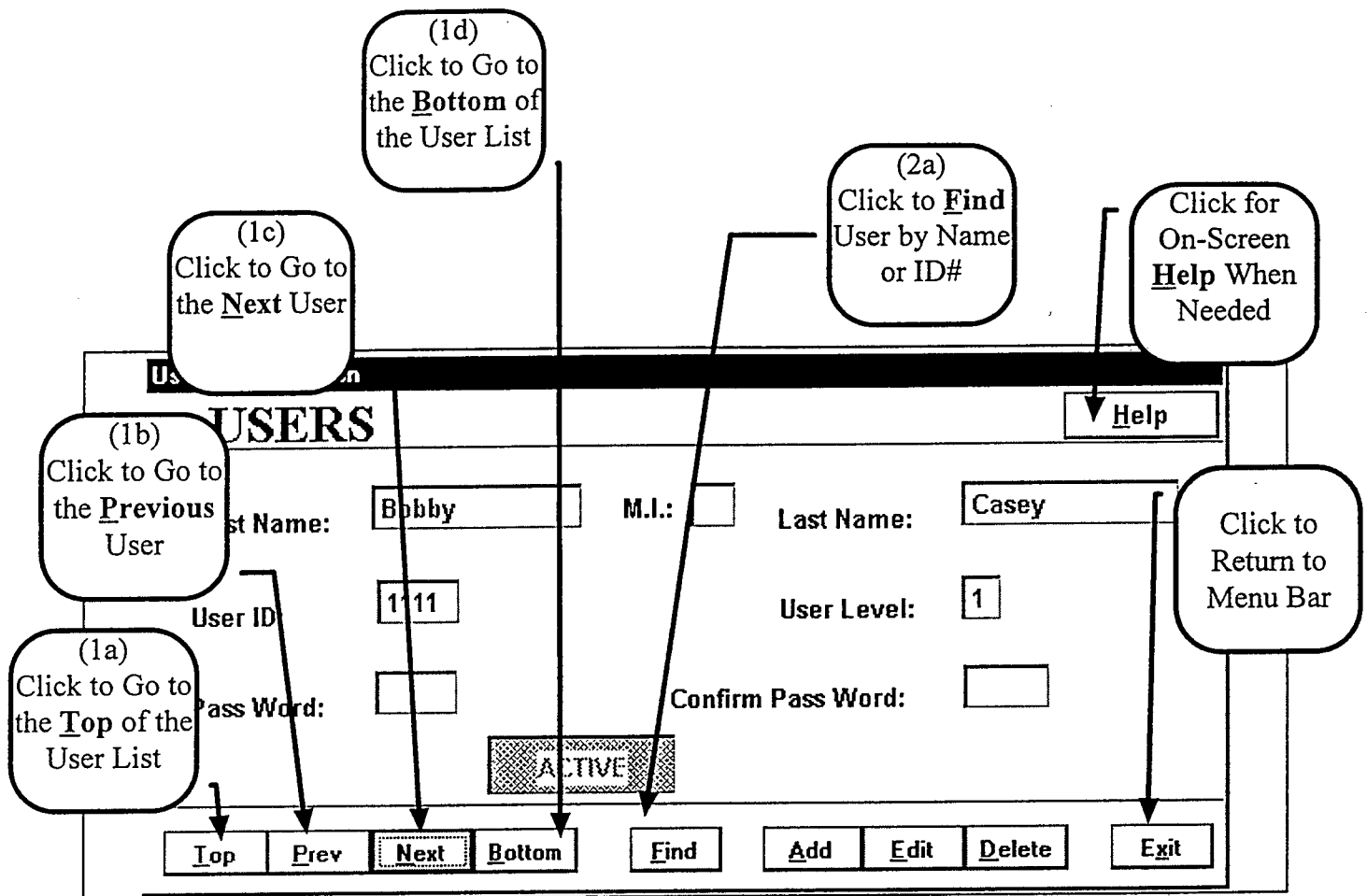


Figure 1. User Administration functions.

How do I scroll through the user list?

(See Figures 2a and 2b)

- Step 1. Click on User Administration from the menu bar.
- Step 2. Click on Add/Edit/Delete Users.
- Step 3. Click on the Top, Previous, Next, or Bottom button to scroll to desired user.

When you have located a specific user, you can edit the information, delete the information, or inactivate a user.

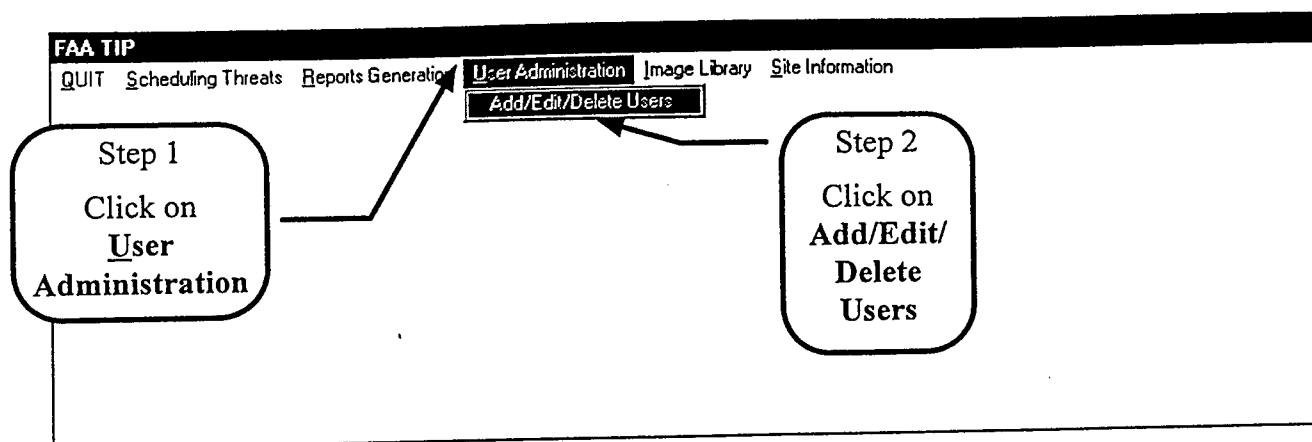


Figure 2a. Scrolling through the TIP user list - steps 1 and 2.

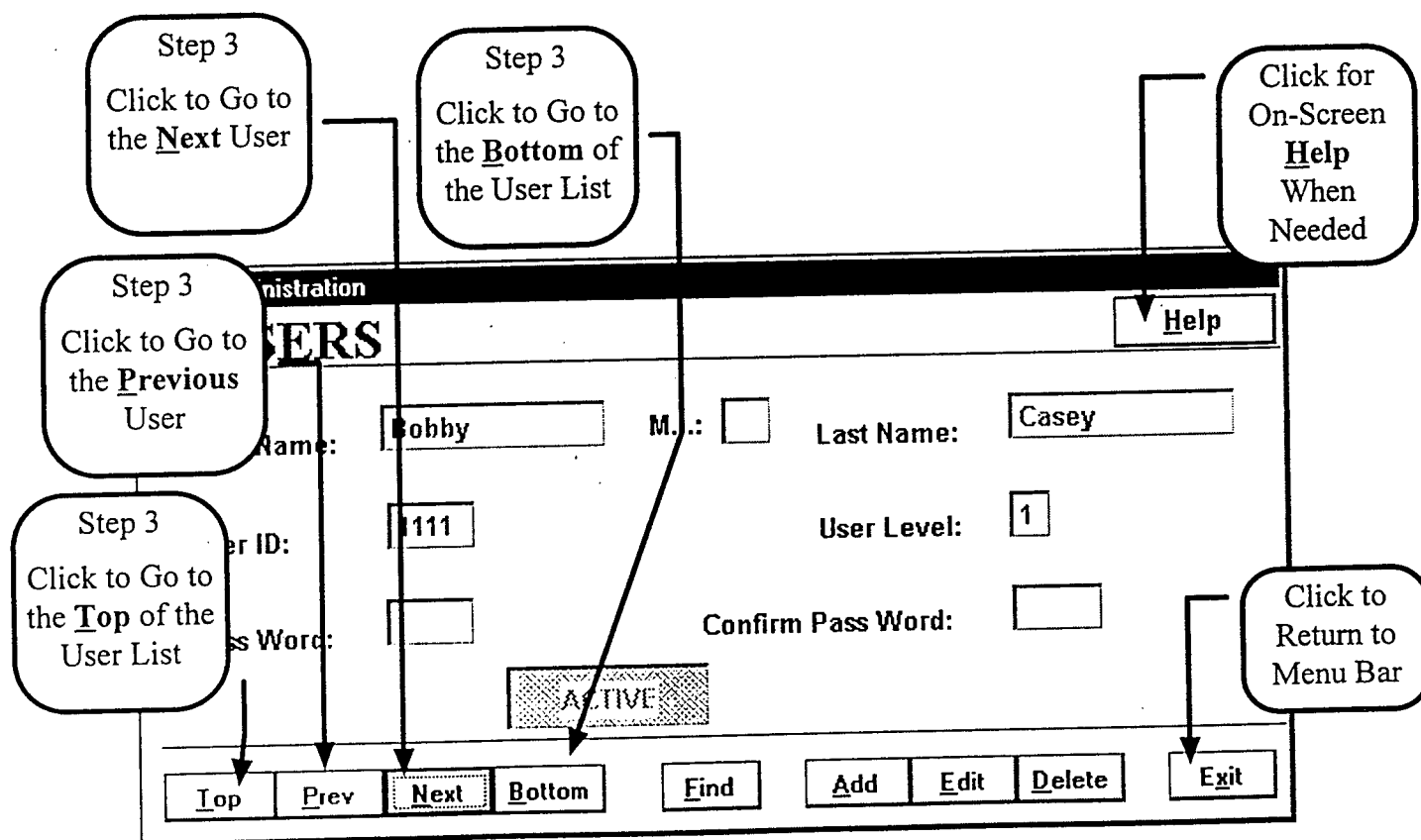


Figure 2b. Scrolling through the TIP user list - step 3.

How do I find a TIP user by name or ID number?

(See Figures 3a, 3b, and 3c)

- Step 1. Click on User Administration from the menu bar.
- Step 2. Click on Add/Edit/Delete Users.
- Step 3. Click on the Find button.
- Step 4. Click on the circle next to Names or Logon IDs.
- Step 5. Click on the user's name or ID number whose record you want to change.
- Step 6. Click on the OK button.

When you have located a specific user and clicked on the OK button, the display will return to the User Administration screen. You can then edit the information, delete the information, or inactivate the user.

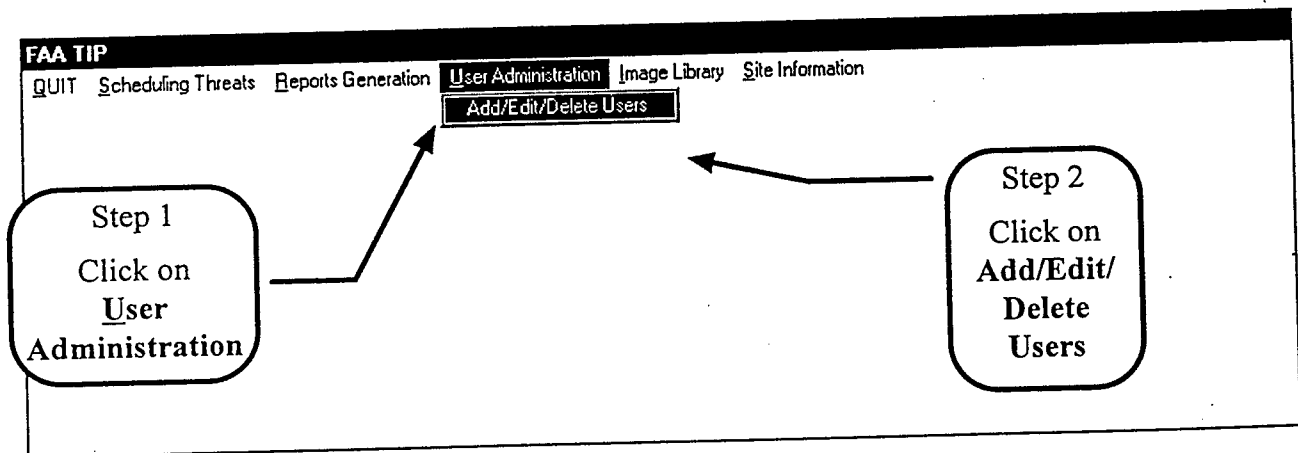


Figure 3a. Finding a user - steps 1 and 2.

User Administration

USERS

Step 3: Click to Find a TIP User

Click for On-Screen Help When Needed

Click to Return to Menu Bar

First Name: Bobby M.I.: ☐ Last Name: Casey

User ID: 1111 User Level: 1

Pass Word: Confirm Pass Word:

ACTIVE

Top Prev Next Bottom Find Add Edit Delete Exit

Figure 3b. Finding a user - step 3.

Step 4: Click to Find by Name or ID Number

Step 5: Click on the User's Name or ID Number

Step 6: Click OK to Return to User Administration Screen

Find

Sorted By:

☒ Names ☐ Logon IDs

OK Cancel

Name	ID	Level
Ames, Thoe	4444	4
Casey, Bobby	1111	4
Dean, James	5555	1
Jones, Susan	3333	3
Smith, Bob	0000	1
Snothy, Dave	2222	2
Williams, Hank	9999	1

Figure 3c. Finding a user - steps 4, 5, and 6.

How do I add a new user?

(See Figures 4a ,4b, and 4c)

Step 1. Click on User Administration from the menu bar.

Step 2. Click on Add/Edit/Delete Users.

Step 3. Click on the Add button.

The information inside of the text boxes will clear and the Add and Edit buttons change to Save and Revert.

Step 4. Type the new user information in the text boxes provided.

Step 5. Click on the Save button to save changes.

OR

Click on the Revert button to abandon changes.

Both options will return you to the **User Administration** screen.

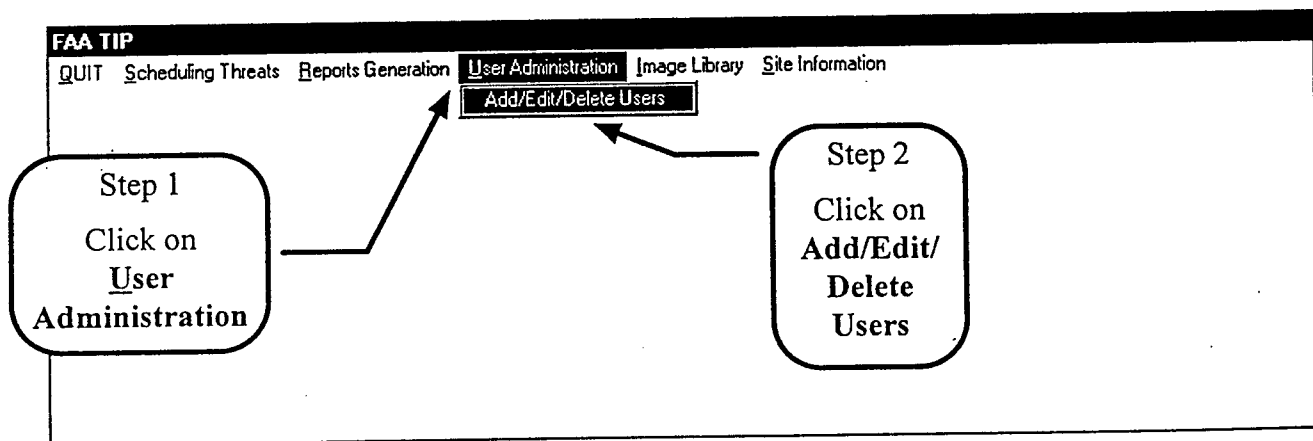


Figure 4a. Adding a new user - steps 1 and 2.

The screenshot shows the 'User Administration' window with the title 'USERS'. It contains several input fields: 'First Name' (Bobby), 'M.I.' (empty), 'Last Name' (Casey), 'User ID' (1111), 'User Level' (1), 'Pass Word' (empty), and 'Confirm Pass Word' (empty). A 'Help' button is in the top right. A 'Next' button is highlighted in the bottom navigation bar. Callouts indicate: Step 3 (Click to Add a User) pointing to the 'Next' button; Step 4 (Type New User Info in Each Box) pointing to the input fields; and a 'Click for On-Screen Help When Needed' pointing to the 'Help' button. A 'Click to Return to Menu Bar' points to the 'Exit' button.

Step 3
Click to Add a User

Step 4
Type New User Info in Each Box

Click for On-Screen Help When Needed

Click to Return to Menu Bar

Figure 4b. Adding a new user - steps 3 and 4.

The screenshot shows the 'User Administration' window with the title 'USERS'. It contains several input fields: 'First Name' (Bobby), 'M.I.' (empty), 'Last Name' (Casey), 'User ID' (1111), 'User Level' (1), 'Pass Word' (empty), and 'Confirm Pass Word' (empty). A 'Help' button is in the top right. A 'Save' button is highlighted in the bottom navigation bar. Callouts indicate: Step 5 (Click to Save or Revert to Abandon) pointing to the 'Save' button; a 'Click for On-Screen Help When Needed' pointing to the 'Help' button; and a 'Click to Return to Menu Bar' pointing to the 'Exit' button.

Step 5
Click to Save or Revert to Abandon

Click for On-Screen Help When Needed

Click to Return to Menu Bar

Figure 4c. Adding a new user - step 5.

How do I change TIP user information?

(See Figures 5a, 5b, and 5c)

Step 1. Click on **U**ser Administration from the menu bar.

Step 2. Click on **A**dd/**E**dit/**D**ele~~t~~e Users.

Step 3. Find and click on the employee to be updated.

Step 4. Click on the **E**dit button.

The information inside of the text boxes will change from gray to black. The **A**dd and **E**dit buttons change to **S**ave and **R**evert.

Step 5. Click on the information to be changed. Type the new information in the text boxes provided.

Step 6. Click on the **S**ave button to save changes.

OR

Click on the **R**evert button to abandon changes.

Both options will return you to the **User Administration** screen.

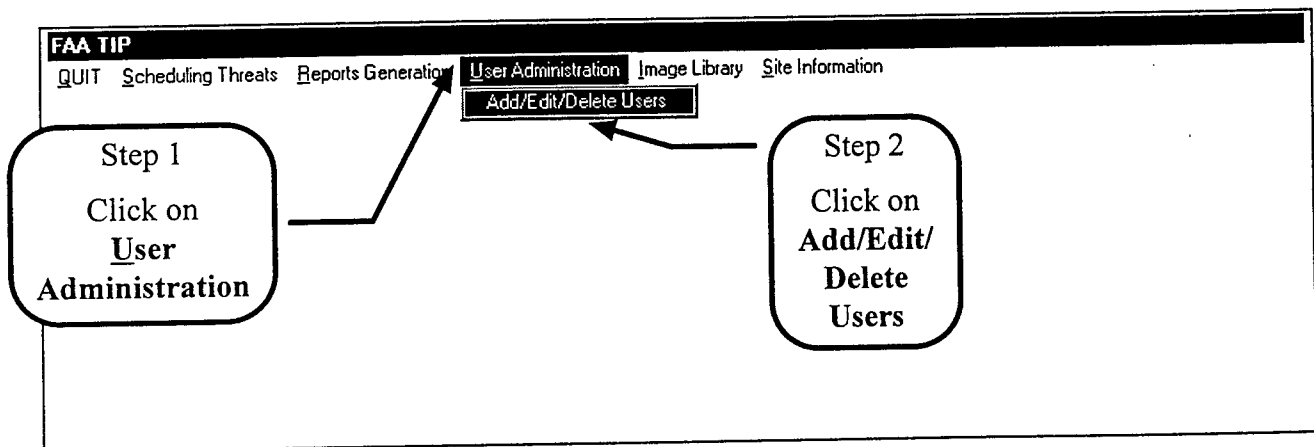


Figure 5a. Editing user information - steps 1 and 2.

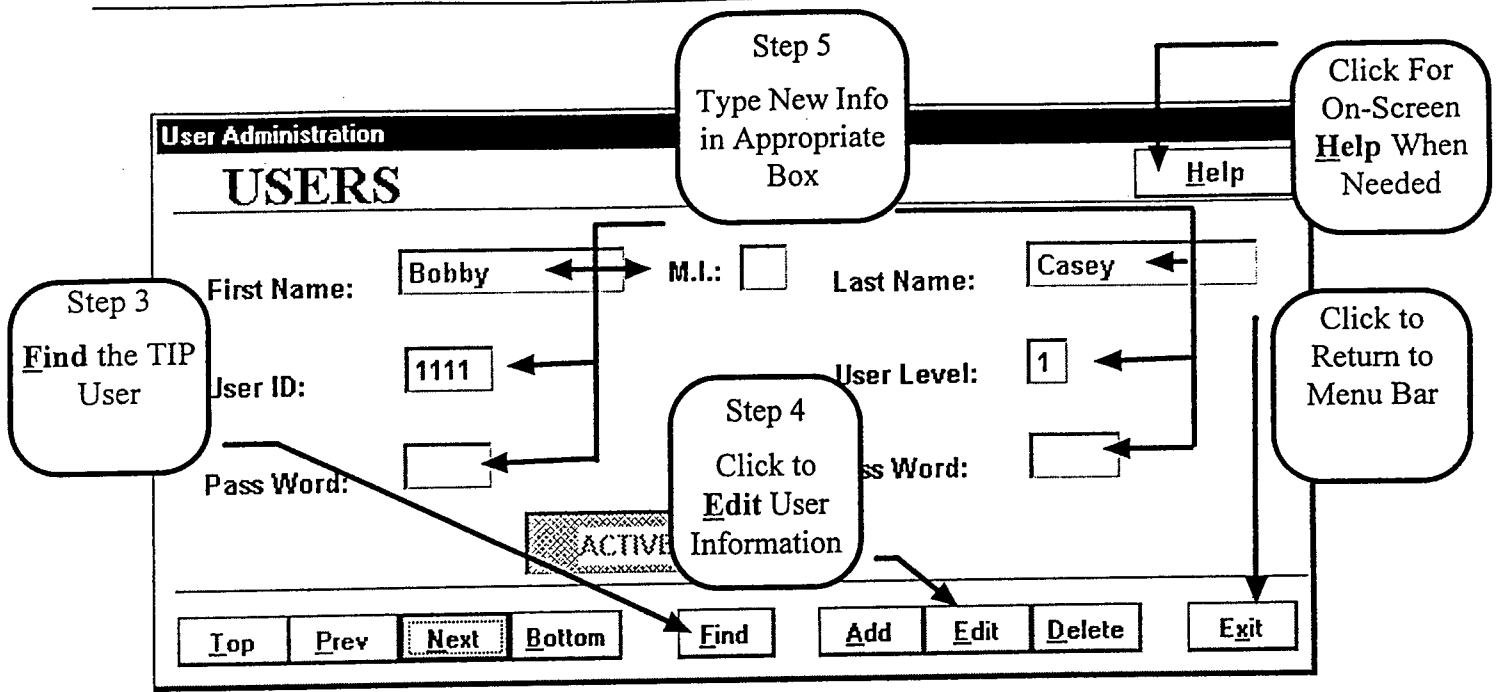


Figure 5b. Editing user information - steps 3, 4, and 5.

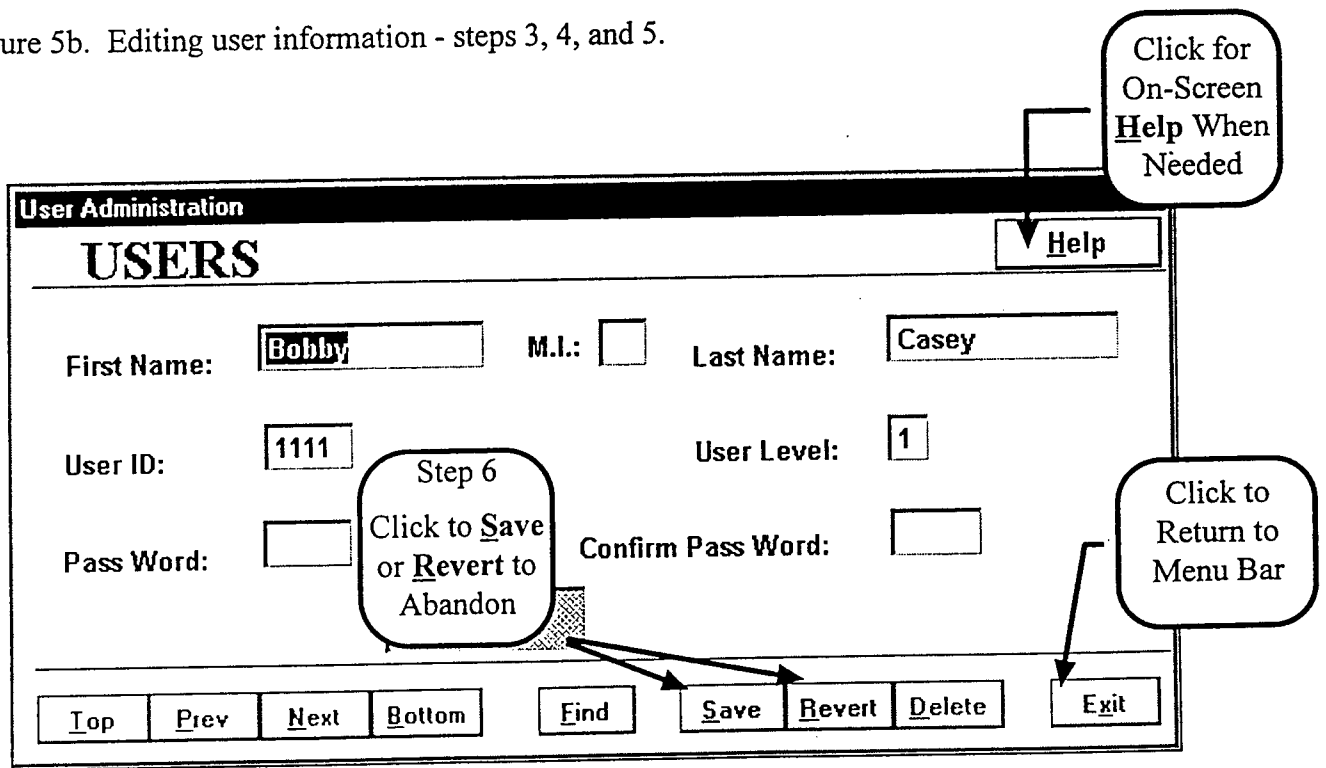


Figure 5c. Editing user information - step 6.

How do I set or change a user's password?

(See Figures 6a, 6b, and 6c)

Step 1. Click on User Administration from the menu bar.

Step 2. Click on **Add/Edit/Delete Users**.

Step 3. Find and click on the employee to be updated.

Step 4. Click on the Edit button.

The information inside of the text boxes will change from gray to black. The Add and Edit buttons change to Save and Revert.

Step 5. Click on the **Pass Word** box. Type in the new password. Press the **Enter** key on the keyboard.

The **Confirm Pass Word:** box will turn gray.

Step 6. Type the new password again.

Step 7. Click on the Save button to save changes.

OR

Click on the Revert button to abandon changes.

Both options will return you to the **User Administration** screen.

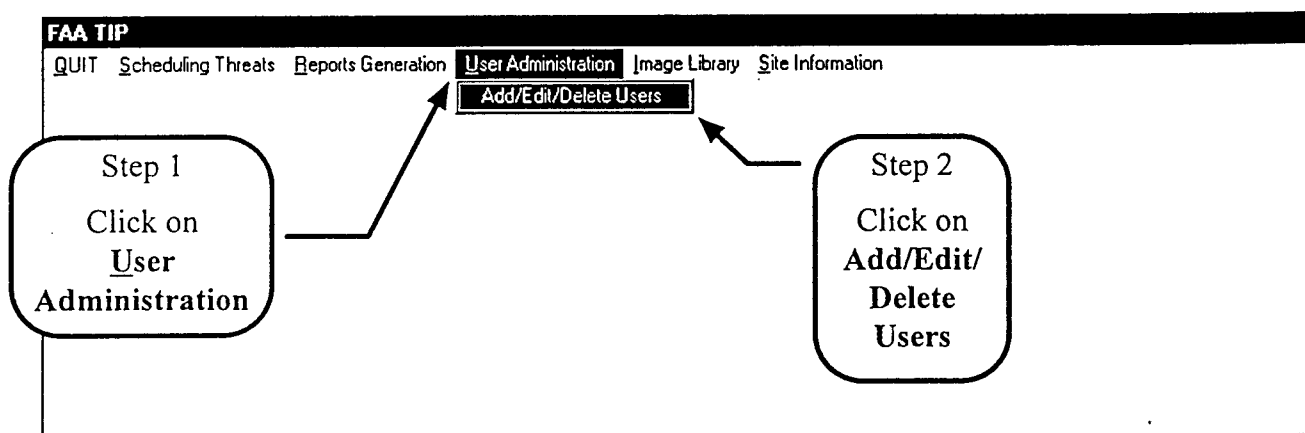


Figure 6a. Setting or changing a user's password - steps 1 and 2.

The screenshot displays the 'User Administration' window with the 'USERS' tab selected. The interface includes a title bar, a menu bar with 'Help', and a main content area with form fields and a button bar. Callouts indicate the following steps:

- Step 3:** Find the TIP User (points to the 'Find' button).
- Step 4:** Click to Edit Password (points to the 'Edit' button).
- Help:** Click for On-Screen Help When Needed (points to the 'Help' button).
- Return:** Click to Return to Menu Bar (points to the 'Exit' button).

The form fields are as follows:

Field	Value
First Name:	Bobby
M.I.:	<input type="checkbox"/>
Last Name:	Casey
User ID:	1111
User Level:	1
Pass Word:	<input type="password"/>
Confirm Pass Word:	<input type="password"/>

The button bar contains: Top, Prev, Next, Bottom, Find, Add, Edit, Delete, Exit. The 'Next' button is highlighted. A status bar at the bottom shows 'ACTIVE'.

Figure 6b. Setting or changing a user's password - steps 3 and 4.

The screenshot displays the 'User Administration' window with the 'USERS' tab selected. The interface includes a title bar, a menu bar with 'Help', and a main content area with form fields and a button bar. Callouts indicate the following steps:

- Step 5:** Type New Password and Press Enter (points to the 'Pass Word' field).
- Step 6:** Retype New Password (points to the 'Confirm Pass Word' field).
- Step 7:** Click to Save or Revert to Abandon (points to the 'Save' and 'Revert' buttons).
- Help:** Click for On-Screen Help When Needed (points to the 'Help' button).
- Return:** Click to Return to Menu Bar (points to the 'Exit' button).

The form fields are as follows:

Field	Value
First Name:	Bobby
M.I.:	<input type="checkbox"/>
Last Name:	Casey
User ID:	1111
User Level:	1
Pass Word:	<input type="password"/>
Confirm Pass Word:	<input type="password"/>

The button bar contains: Top, Prev, Next, Bottom, Find, Save, Revert, Delete, Exit. The 'Save' button is highlighted. A status bar at the bottom shows 'ACTIVE'.

Figure 6c. Setting or changing a user's password - steps 5, 6, and 7.

How do I set or change a user's security access level?

(See Figures 7a, 7b, and 7c)

- Step 1. Click on **U**ser Administration from the menu bar.

Step 2. Click on **A**dd/Edit/Delete Users.

Step 3. Find and click on the employee to be updated.

Step 4. Click on the **E**dit button.

The data inside the information boxes will change from gray to black. The **A**dd and **E**dit buttons change to **S**ave and **R**evert.

- Step 5. Click on the **U**ser Level box. Type in the new level number. Press the **E**nter key on the keyboard.

Step 6. Click on the **S**ave button to save changes.
OR
Click on the **R**evert button to abandon changes.

Both options will return you to the **User Administration** screen.

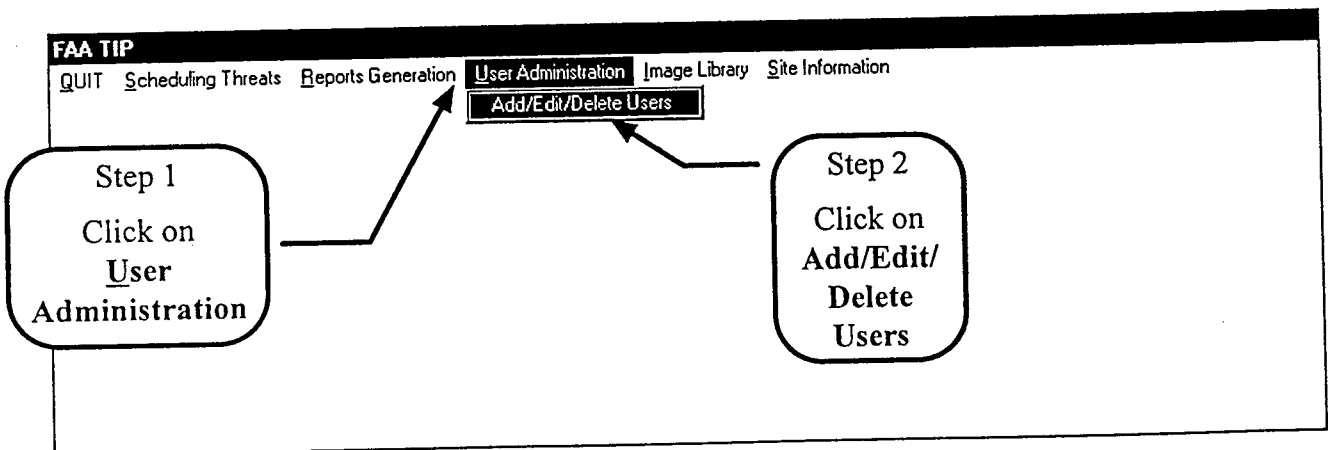


Figure 7a. Setting or changing a user's security access level - steps 1 and 2.

The screenshot shows the 'User Administration' window with the title 'USER'. The interface includes the following elements:

- Form Fields:**
 - First Name: Bobby
 - M.I.: []
 - Last Name: Casey
 - User ID: 1111
 - User Level: 1
 - Pass Word: []
 - Confirm Pass Word: []
- Buttons:** Top, Prev, Next, Bottom, Find, Add, Edit, Delete, Exit.
- Annotations:**
 - Step 3:** Find the TIP User (arrow points to the User ID field).
 - Step 4:** Click to Edit User Information (arrow points to the Edit button).
 - ACTIVE:** A shaded box with the word 'ACTIVE' is located below the Password field.
 - Help:** Click for On-Screen Help When Needed (arrow points to the Help button).
 - Return:** Click to Return to Menu Bar (arrow points to the Exit button).

Figure 7b. Setting or changing a user's Security Access Level - steps 3 and 4.

The screenshot shows the 'User Administration' window with the title 'USERS'. The interface includes the following elements:

- Form Fields:**
 - First Name: Bobby
 - M.I.: []
 - Last Name: Casey
 - User ID: 1111
 - User Level: 1
 - Pass Word: []
 - Confirm Pass Word: []
- Buttons:** Top, Prev, Next, Bottom, Find, Save, Revert, Delete, Exit.
- Annotations:**
 - Step 5:** Click on User Level Box and Type New Level Number; Press Enter (arrow points to the User Level field).
 - Step 6:** Click to Save or Revert to Abandon (arrows point to the Save and Revert buttons).
 - Help:** Click for On-Screen Help When Needed (arrow points to the Help button).
 - Return:** Click to Return to Menu Bar (arrow points to the Exit button).

Figure 7c. Setting or changing a user's security access level - steps 5 and 6.

How do I delete a user?

Note: Information in the database is deleted two months after it has been downloaded. Users may only be deleted if they have never logged in or when all database records involving that individual no longer reside in the system. If a user has logged into the TIP system, follow the instructions for changing a user to an inactive status.

If a TIP user has been deleted, the action cannot be undone. The user information must be entered again following the steps for adding a user.

(See Figures 8a and 8b)

Step 1. Click on **User Administration** from the menu bar.

Step 2. Click on **Add/Edit/Delete Users**.

Step 3. Find and click on the TIP user to be deleted.

Step 4. Click on the **Delete** button.

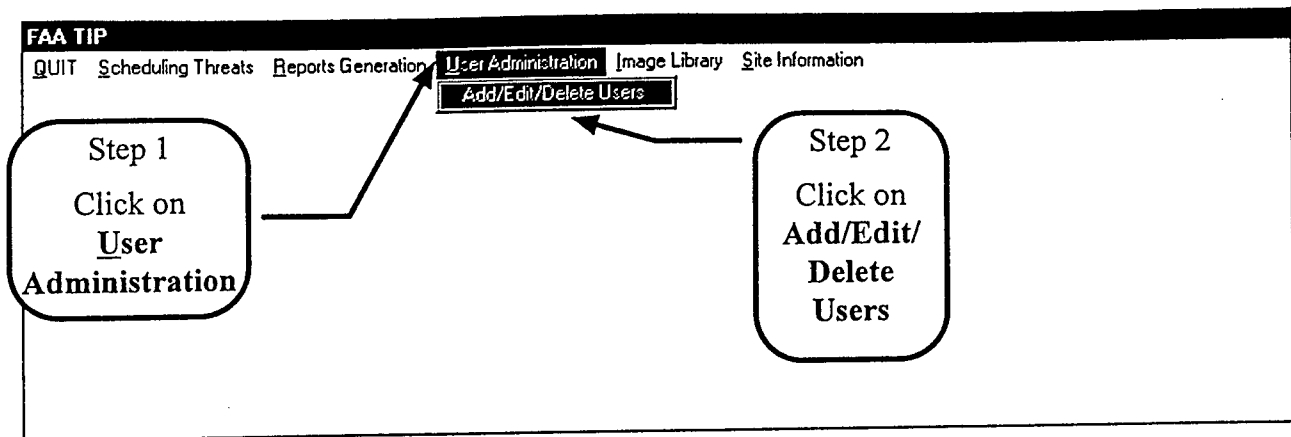


Figure 8a. Deleting a user - steps 1 and 2.

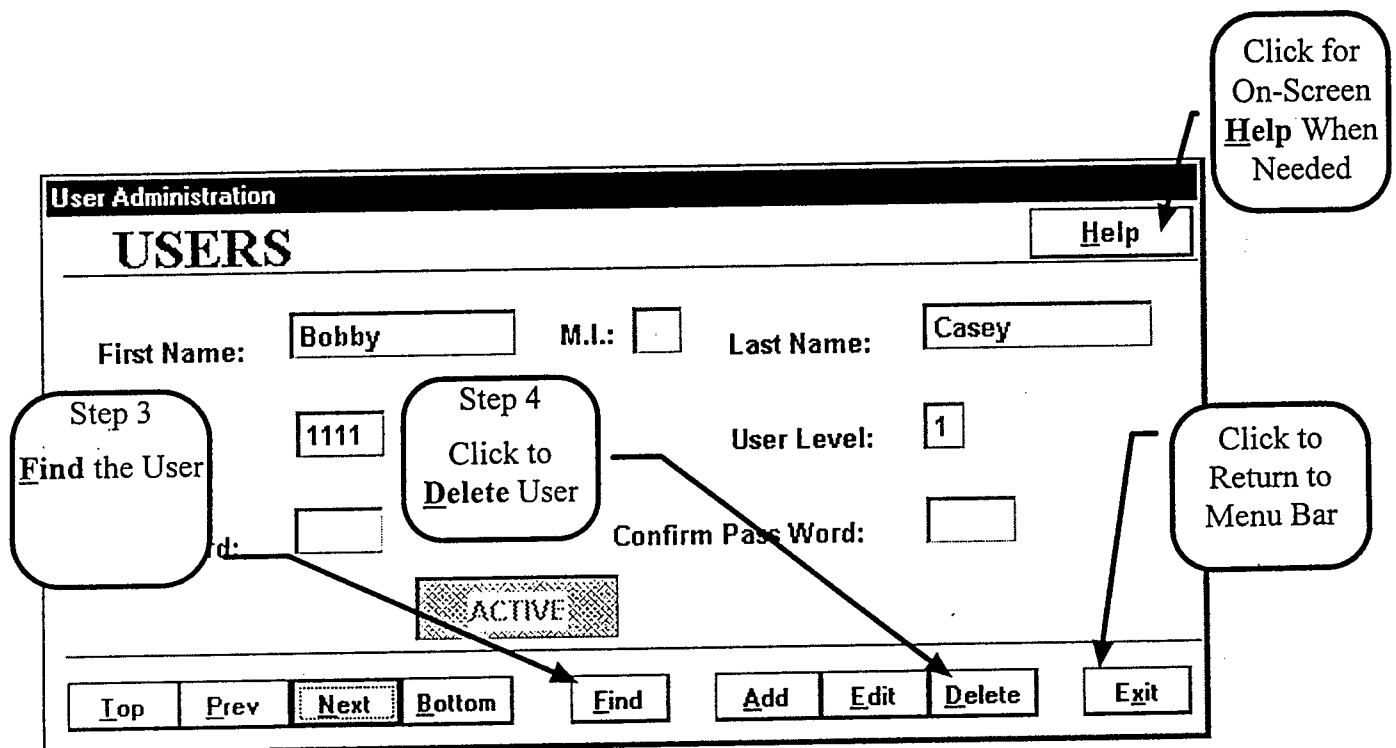


Figure 8b. Deleting a user - steps 3 and 4.

How do I change an active user to inactive status?

(See Figures 9a, 9b, and 9c)

- Step 1. Click on User Administration from the menu bar.
- Step 2. Click on **Add/Edit/Delete Users**.
- Step 3. Find and click on the TIP user to be inactivated.
- Step 4. Click on the Edit button.

The Add and Edit buttons change to Save and Revert.

- Step 5. Click on the Active box. The box will automatically change to **Inactive**.
- Step 6. Click on the Save button to save changes.
OR
Click on the Revert button to abandon changes.

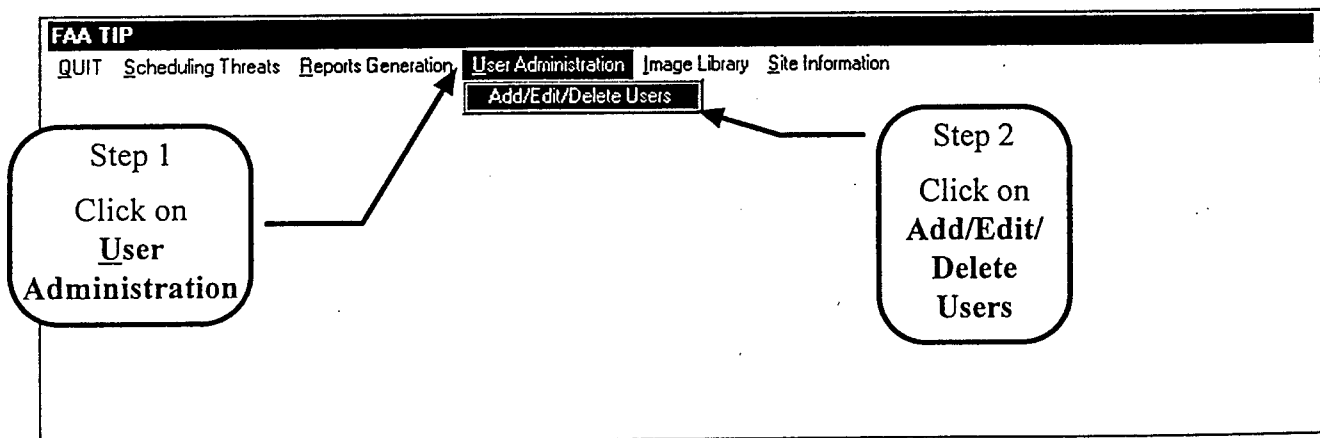


Figure 9a. Changing the status of a user - steps 1 and 2.

The screenshot shows the 'User Administration' window with the title 'USERS'. It contains several input fields: 'First Name:', 'M.I.', 'Last Name:' (with 'Casey' entered), 'User ID:' (with '1111' entered), 'User Level:' (with '1' entered), 'Pass Word:', and 'Confirm Pass Word:'. A status box labeled 'ACTIVE' is visible. At the bottom is a menu bar with buttons: 'Top', 'Prev', 'Next', 'Bottom', 'Find', 'Add', 'Edit', 'Delete', and 'Exit'. A 'Help' button is in the top right. Annotations include: 'Step 3 Find the User' pointing to the 'Find' button; 'Step 4 Click to Edit Status' pointing to the 'Edit' button; 'Click for On-Screen Help When Needed' pointing to the 'Help' button; and 'Click to Return to Menu Bar' pointing to the 'Exit' button.

Figure 9b. Changing the status of a user - steps 3 and 4.

The screenshot shows the 'User Administration' window with the title 'USERS'. It contains several input fields: 'First Name:' (with 'Bobby' entered), 'M.I.', 'Last Name:' (with 'Casey' entered), 'User ID:' (with '1111' entered), 'User Level:' (with '1' entered), 'Pass Word:', and 'Confirm Pass Word:'. A status box labeled 'ACTIVE' is visible. At the bottom is a menu bar with buttons: 'Top', 'Prev', 'Next', 'Bottom', 'Find', 'Save', 'Revert', 'Delete', and 'Exit'. A 'Help' button is in the top right. Annotations include: 'Step 5 Click to Change From Active to Inactive' pointing to the 'ACTIVE' status box; 'Step 6 Click to Save or Revert to Abandon' pointing to the 'Save' and 'Revert' buttons; and 'Click to Return to Menu Bar' pointing to the 'Exit' button.

Figure 9c. Changing the status of a user - steps 5 and 6.

Management of the TIP Image Library

What is the TIP Image Library?

The TIP Image Library is a collection of threat images. The images are organized by threat category (e.g., bomb, knife, and gun), then by threat subcategory (e.g., bomb - Improvised Explosive Device). You may view the images as they are seen by screeners during the baggage X-ray screening process.

What topics will be covered in this section?

1. Contents and functions of the Image Library
2. Setting TIP to include or exclude specific threat images in the presentation
 - ◇ To do this, your options are to
 - ⇒ Locate a specific threat
 - ⇒ Include a specific threat in the presentation schedule
 - ⇒ Include all threats within a threat category and subcategory
 - ⇒ Exclude a specific threat from the presentation schedule
 - ⇒ Exclude all threats within a threat category and subcategory
3. Viewing a threat image on screen
4. Adding a new threat image to the library
5. Downloading a threat image from the library
6. Uploading a new threat from a disk
7. Deleting a threat from the library
8. Adding a new threat subcategory

What new terms will I need to know for this section?

- **Threat category** - General threat types (e.g., bombs, combined threat images, guns, HAZMAT, and knives)
- **Threat subcategory** - Specific types of threats within each threat category (For example, the Bomb category is divided into three subcategories: Improvised Explosive Device; Nuclear, Biological, and Chemical; and Conventional.)

How do I locate a specific threat in the TIP Image Library?

(See Figures 10a and 10b)

Step 1. Click on **Image Library** on the menu bar.

Step 2. Click on **Navigate/Add/Download/Upload/Delete/Include/Exclude Threats**.

Step 3. Click on the desired category.

Step 4. Click on the desired subcategory.

Step 5. Scroll to and click on the desired threat.

After you have located a threat within the Threat Image Library, you can include it, exclude it from the TIP presentation sequence, or view the image.

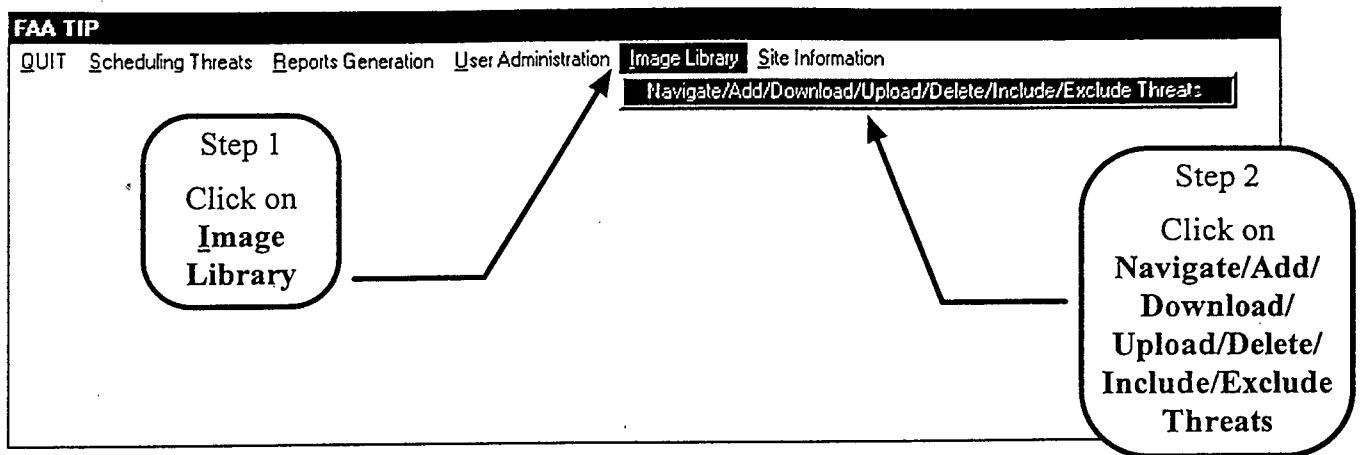


Figure 10a. Locating a specific threat - steps 1 and 2.

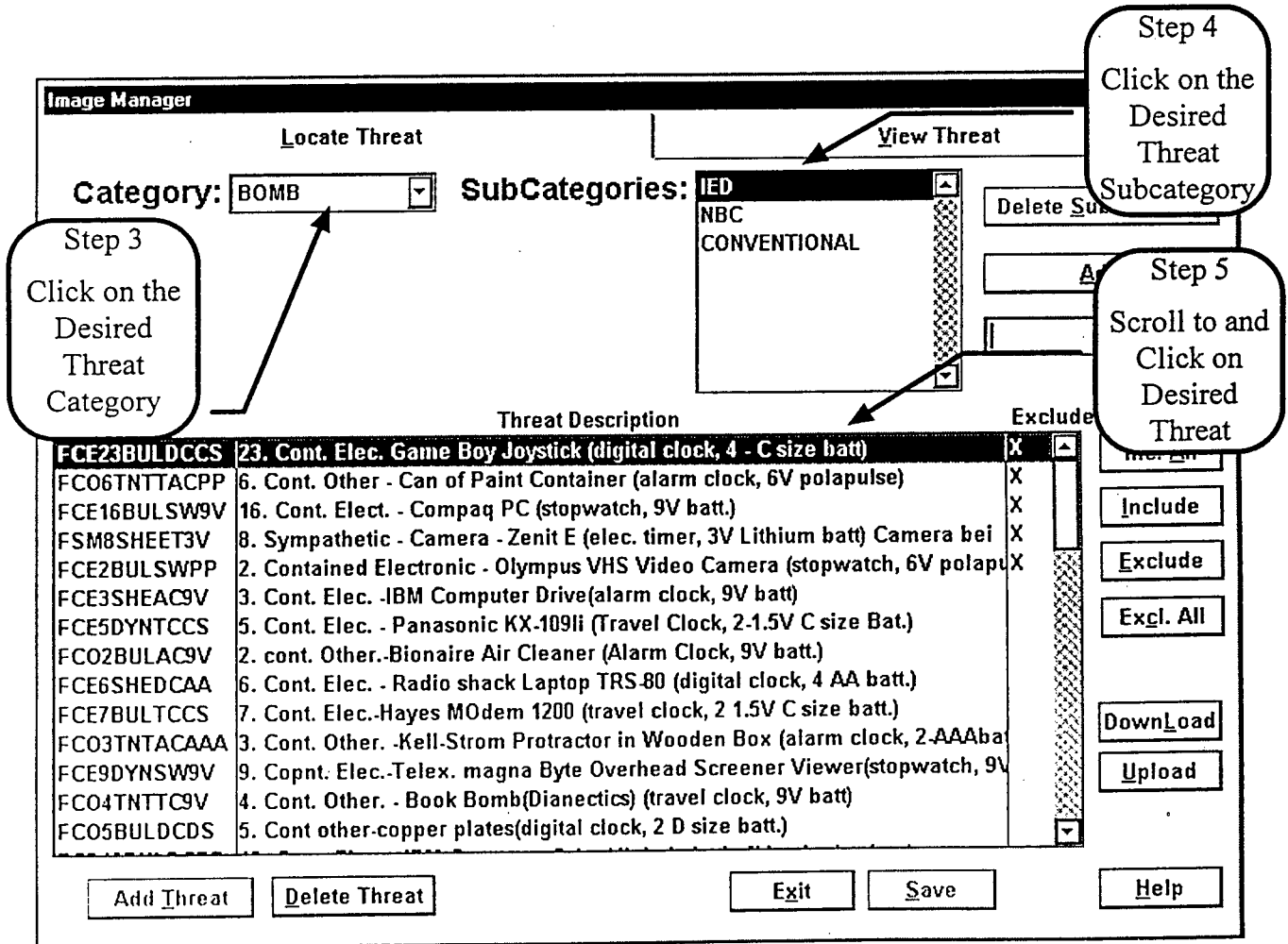


Figure 10b. Locating a specific threat - steps 3, 4, and 5.

How do I set TIP to include specific threats?

(See Figures 11a and 11b)

- Step 1. Click on **I**mage Library on the menu bar.

Step 2. Click on **N**avigate/**A**dd/**D**ownload/**U**pload/**D**elete/**I**nclude/**E**xclude Threats.

Step 3. Click on the desired category.

Step 4. Click on the desired subcategory.

Step 5. Scroll to and click on the desired threat.

Step 6. Click on the **I**nclude button.

Repeat steps 3, 4, 5, and 6 for each threat to be included.

- Step 7. Click on the **S**ave button to save changes.
OR
Click on the **E**xit button to abandon changes.

Note: If there is no X in the **E**xclude column, TIP will present the threat image. If there is an X in the **E**xclude column, TIP will not present that specific threat image.

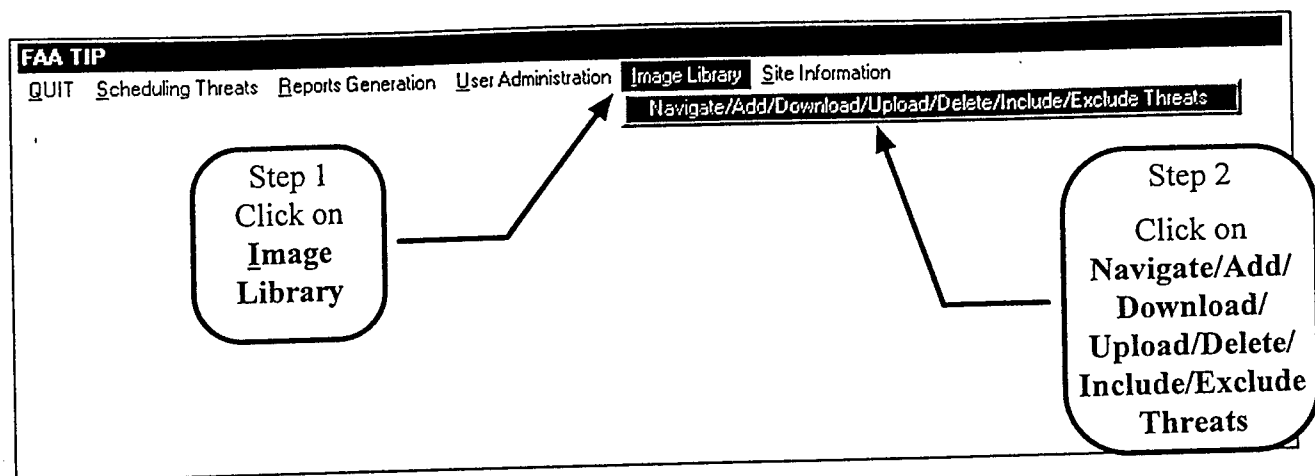


Figure 11a. Including a specific threat - steps 1 and 2.

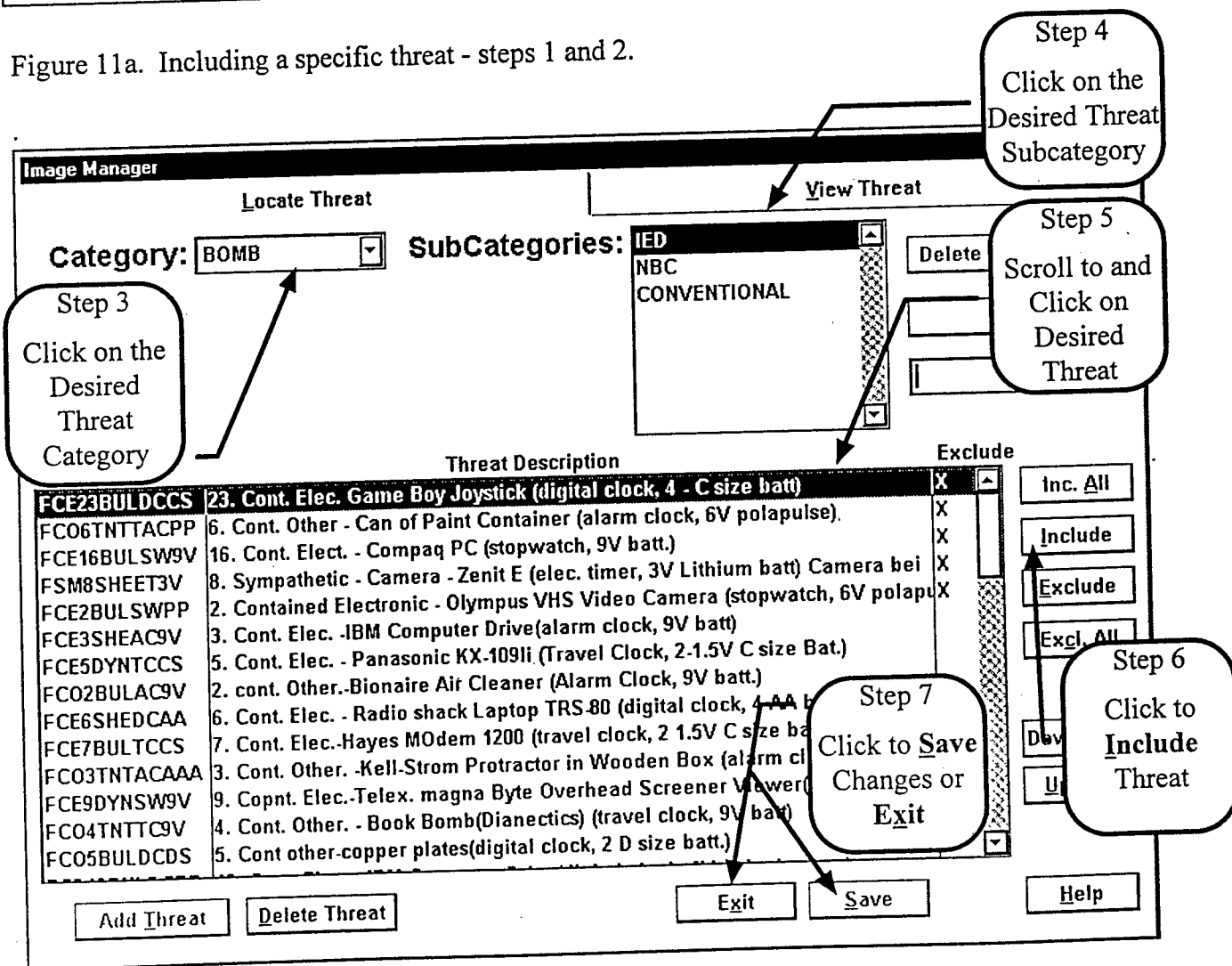


Figure 11b. Including a specific threat - steps 3, 4, 5, 6, and 7.

How do I set TIP to include all threat images of a specific category and subcategory?

(See Figures 12a and 12b)

Step 1. Click on **I**mage Library on the menu bar.

Step 2. Click on **N**avigate/**A**dd/**D**ownload/**U**pload/**D**elete/**I**nclude/**E**xclude
Threats.

Step 3. Click on the desired category.

Step 4. Click on the desired subcategory.

Step 5. Click on the **I**nc. **A**ll button.

Note: This operation must be accomplished for each category and subcategory to be excluded from the presentation.

Repeat step 3, 4, and 5 for each category and subcategory to be included.

Step 6. Click on the **S**ave button to save changes.

OR

Click on the **E**xit button to abandon changes.

Note: If there is no X in the **E**xclude column, TIP will present the threat image. If there is an X in the **E**xclude column, TIP will not present that specific threat image.

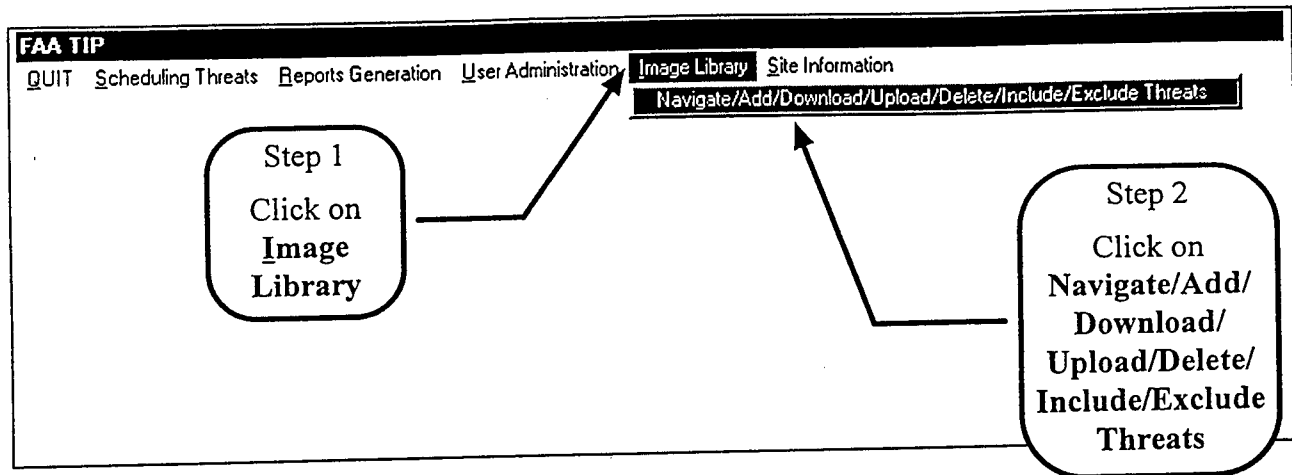


Figure 12a. Including all threat images of a specific category and subcategory - steps 1 and 2.

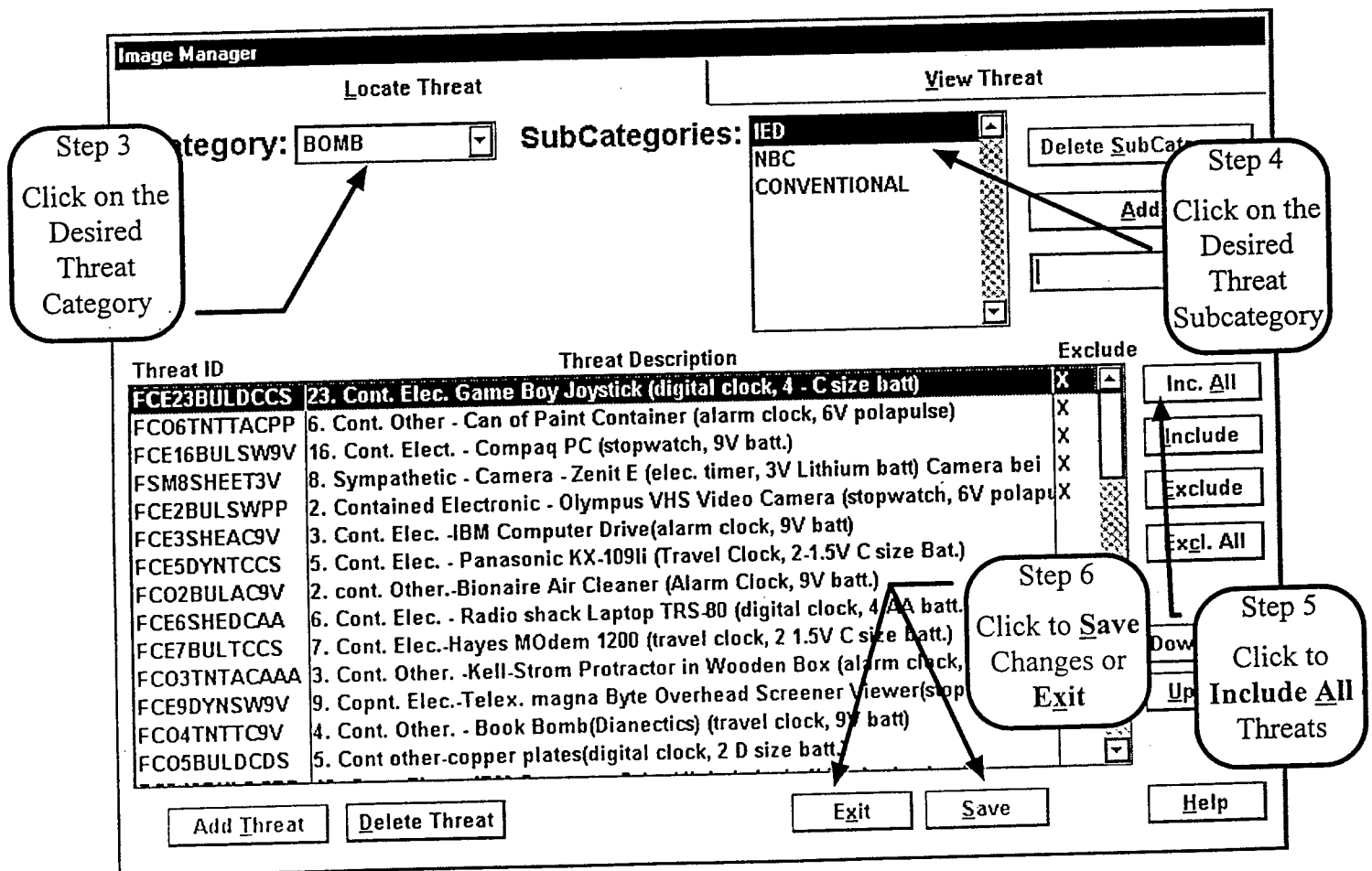


Figure 12b. Including all threat images of a specific category and subcategory - steps 3, 4, 5, and 6.

How do I set TIP to exclude a specific threat image?

(See Figures 13a and 13b)

Step 1. Click on **I**mage Library on the menu bar.

Step 2. Click on **N**avigate/**A**dd/**D**ownload/**U**pload/**D**ele~~t~~e/**I**nclude/**E**xclude
Threats.

Step 3. Click on the desired category.

Step 4. Click on the desired subcategory.

Step 5. Click on the desired threat.

Step 6. Click on the **E**xclude button.

An X will be displayed in the **E**xclude column next to the specific threat description.

Repeat steps 3, 4, 5, and 6 for each threat to be excluded.

Step 7. Click on the **S**ave button to save changes.

OR

Click on the **E**xit button to abandon changes.

Note: If there is no X in the **E**xclude column, TIP will present the threat image. If there is an X in the **E**xclude column, TIP will not present that specific threat image.

The excluded threat images remain part of the library but will not be presented.

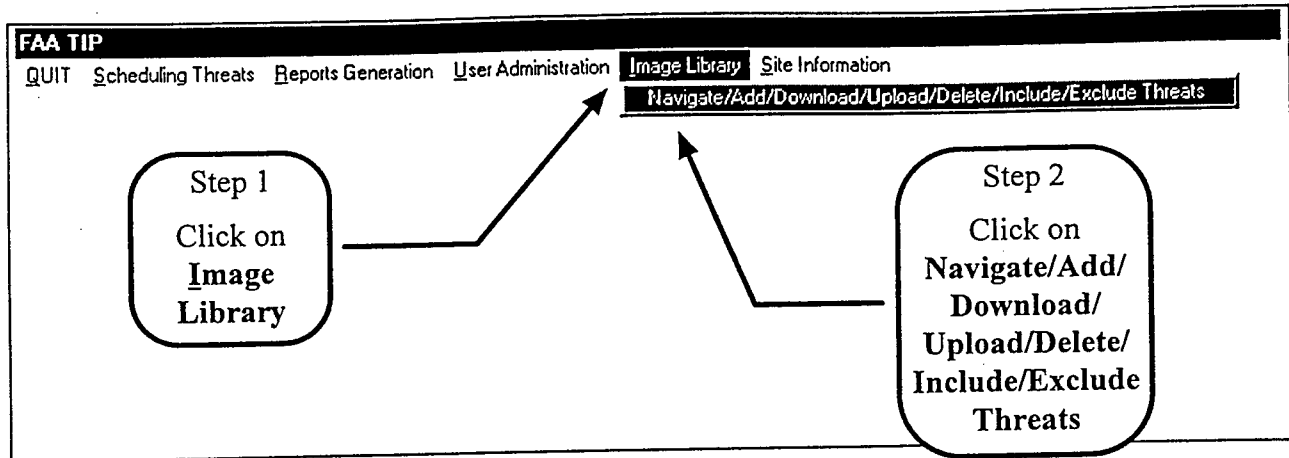


Figure 13a. Excluding a threat image from the TIP presentation - steps 1 and 2.

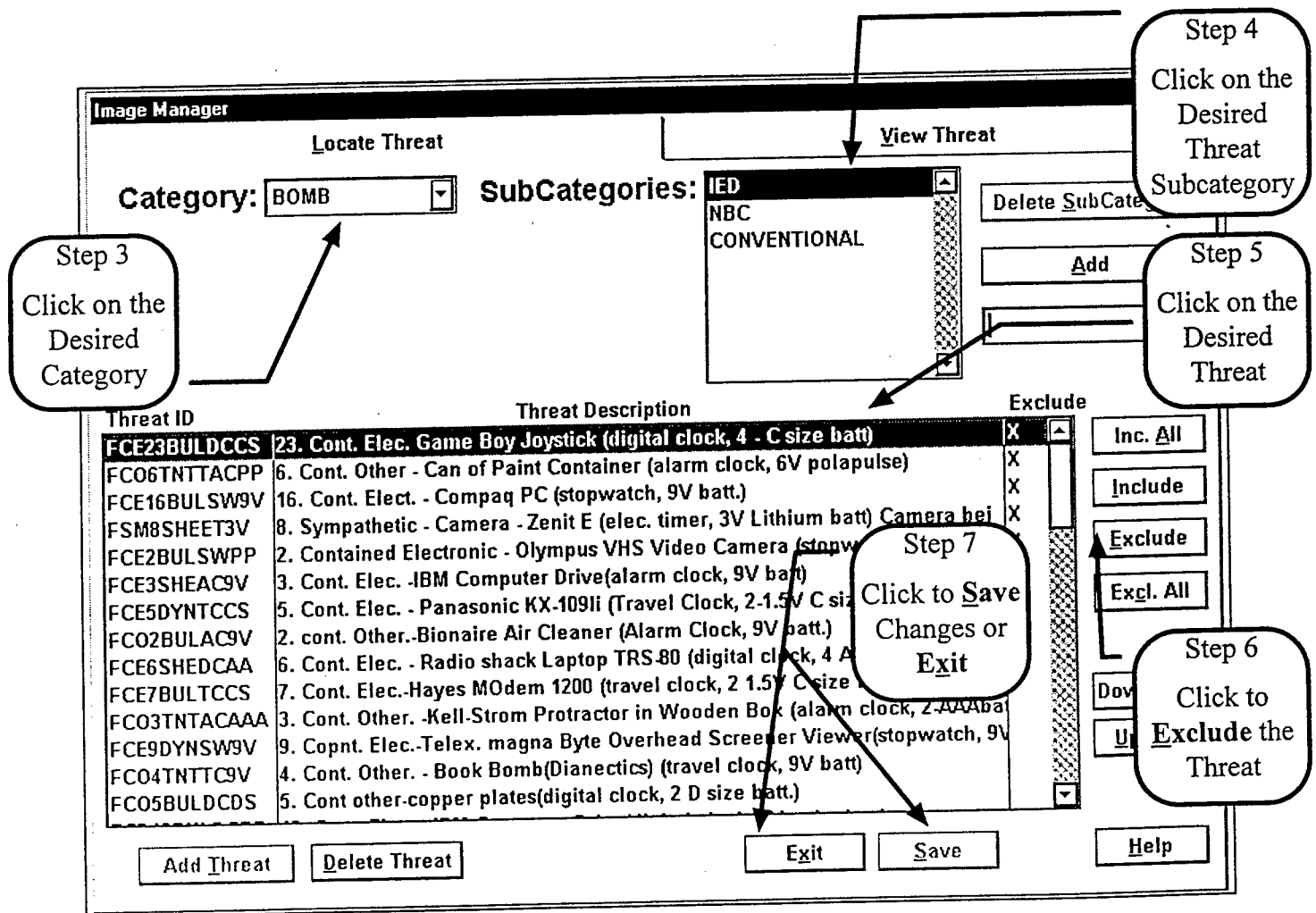


Figure 13b. Excluding a threat image from the TIP presentation - steps 3, 4, 5, 6, and 7.

How do I set TIP to exclude all threat images of a specific category and subcategory?

As an alternative to the following steps, the category and subcategory can be set to 0% in the **Category/SubCategory Percentages** window.

(See Figures 14a and 14b)

- Step 1. Click on **I**mage Library on the menu bar.
- Step 2. Click on **N**avigate/**A**dd/**D**ownload/**U**pload/**D**elete/**I**nclude/**E**xclude Threats.
- Step 3. Click on the desired category.
- Step 4. Click on the desired subcategory.
- Step 5. Click on the **E**xcl. All button.

Xs will be displayed in the **E**xclude column next to the threat descriptions.

Note: This operation must be accomplished for each category and subcategory to be excluded from the presentation.

Repeat steps 3, 4, and 5 for each category and subcategory to be excluded.

- Step 6. Click on the **S**ave button to save changes.
OR
Click on the **E**xit button to abandon changes.

Note: If there is no X in the **E**xclude column, TIP will present the threat image. If there is an X in the **E**xclude column, TIP will not present that specific threat image.

The excluded threat images remain part of the library but will not be presented.

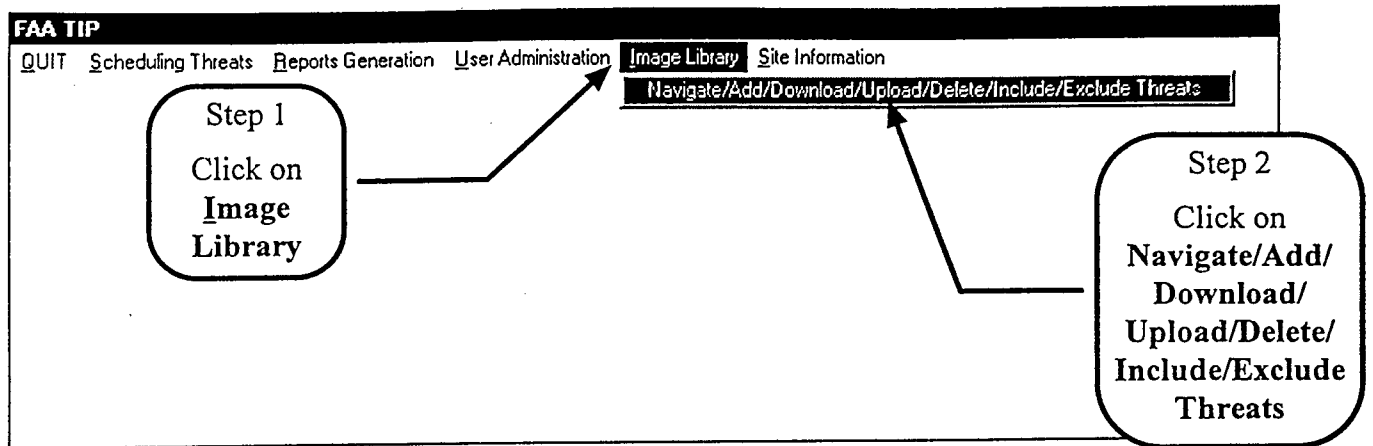


Figure 14a. Excluding all threats in a specific category and subcategory - steps 1 and 2.

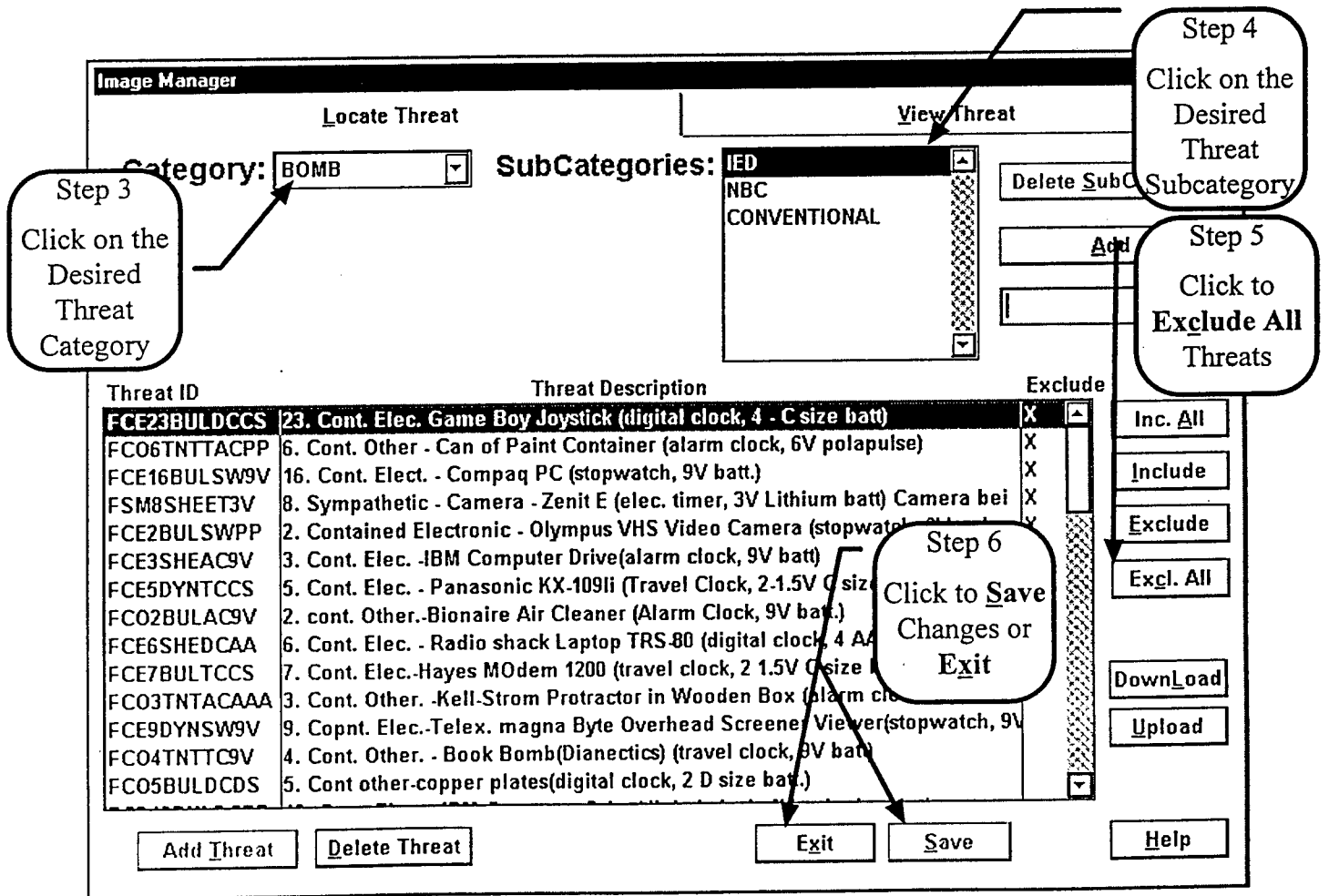


Figure 14b. Excluding all threats in a specific category and subcategory - steps 3, 4, 5, and 6.

How do I view a threat image on the screen?

(See Figures 15a and 15b)

This feature allows you to view a selected threat image as it will appear to the screener during the X-ray baggage screening process.

- Step 1. Click on **I**mage Library on the menu bar.

Step 2. Click on **N**avigation-**T**hreat **I**nclusion/**E**xclusion.

Step 3. Click on the desired category.

Step 4. Click on the desired subcategory.

Step 5. Click on the desired threat.

Step 6. Click on the **V**iew Threat tab.

Note: The selected threat image will be projected on the monitor. When you have finished viewing the threat, press the **Escape** key on the keyboard to return to the **Image Manager** screen.

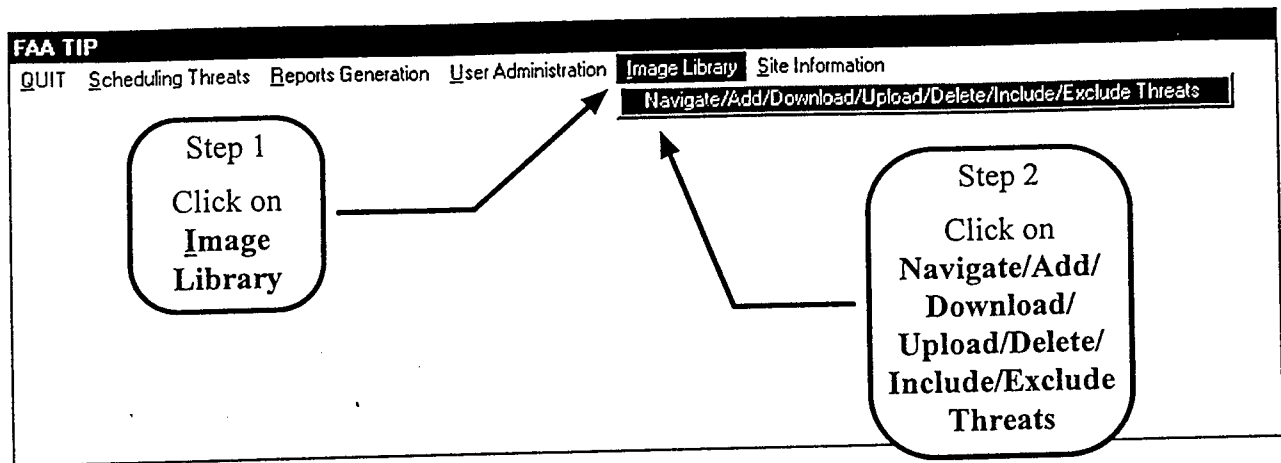


Figure 15a. Viewing threat images - steps 1 and 2.

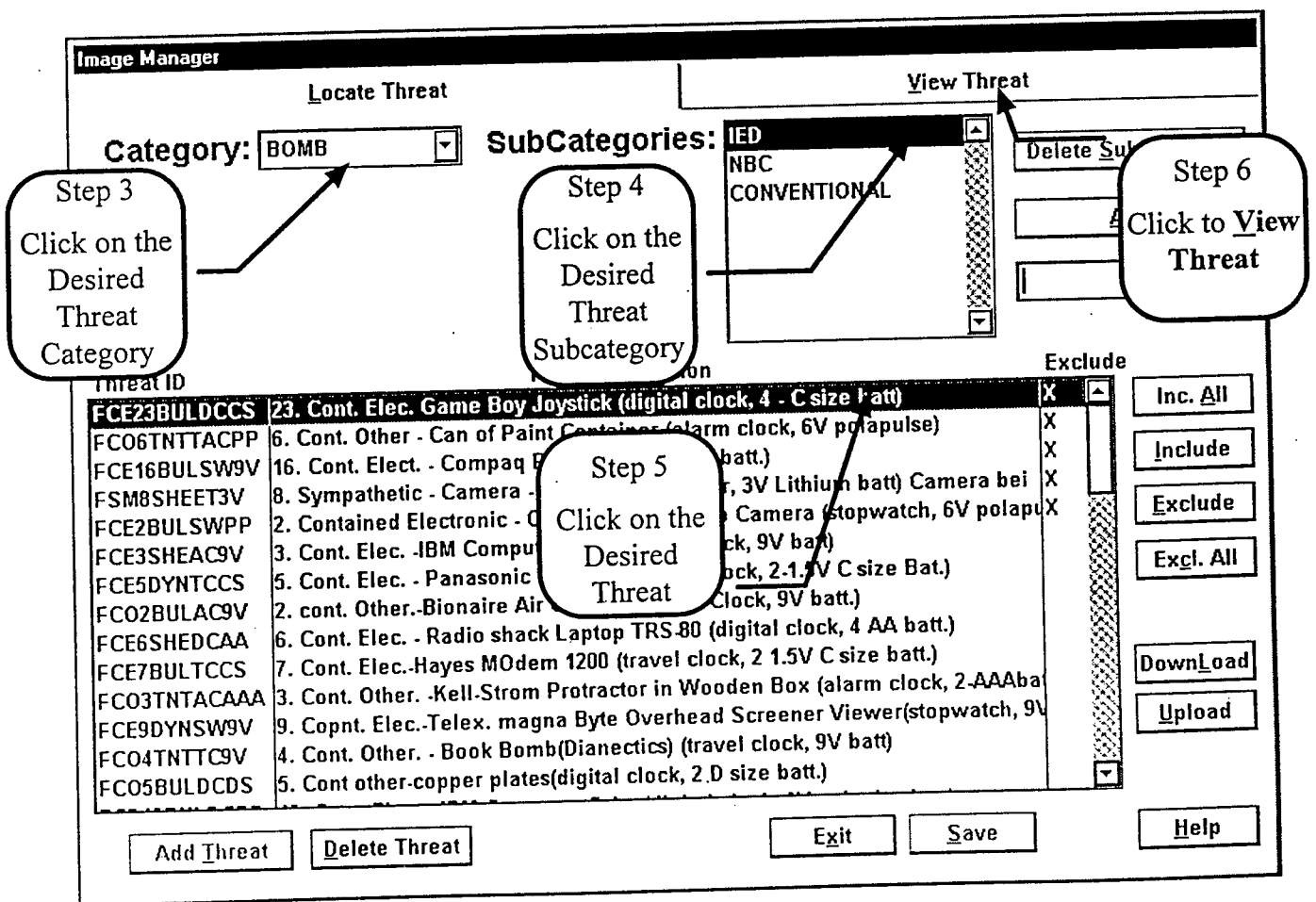


Figure 15b. Viewing threat images - steps 3, 4, 5, and 6.

How do I add a new threat into the Image Library?

(See Figures 16a, 16b, and 16c)

There are two methods for including an image to the Image Library. The first is to scan the image from the X-ray machine and the second is to upload it from a disk.

Two steps are required to add new threats to the Image Library by scanning, you need to

1. capture the threat images using the Image Capture program, and
2. add the threats to the database library using the **Add Threat** button in the **Image Manager** window.

The following steps are for capturing the image.

- Step 1. Click on **Image Capture** icon on the Windows desktop.

Step 2. Enter the threat name in the **Image Capture** window.

Step 3. Click on the **Start Scan** button.

Step 4. Click on the **Exit** button when the scan is finished.

The following step are for adding the image to the Image Library.

- Step 1. Click on **Image Library** on the menu bar.

Step 2. Click on **Navigate/Add/Download/Upload/Delete/Include/Exclude Threats**.

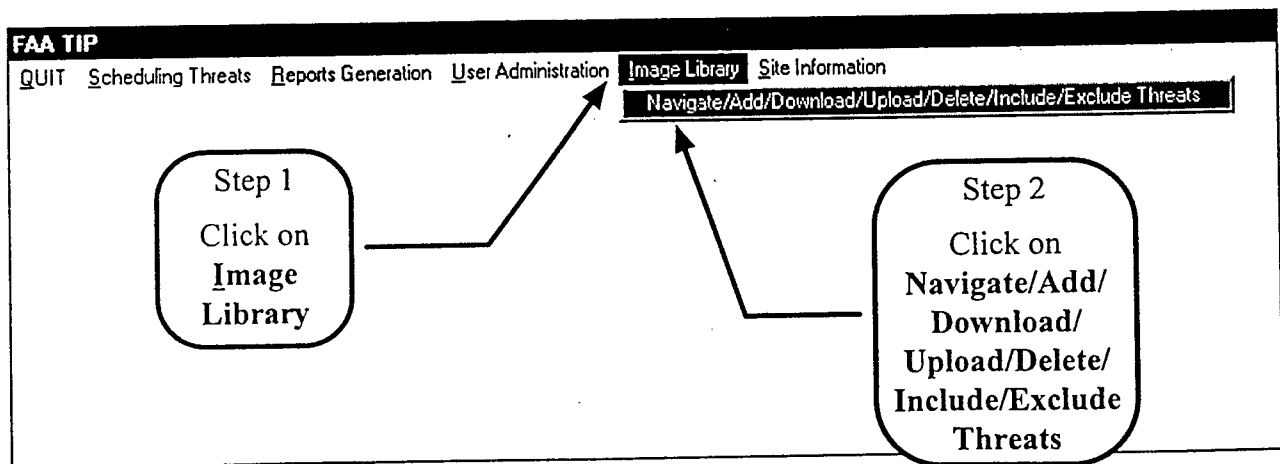


Figure 16a. Adding a new threat image - steps 1 and 2.

Step 3. Click on the appropriate category.

Step 4. Click on the appropriate subcategory.

Step 5. Click on the **Add Threat** button. (You will be asked to confirm the category and subcategory of the new threat.)

Step 6. Type in the **Nomenclature**, **Description**, and **Path\Filename** of the new threat in the **New Threat** window.

Step 7. Click on the **OK** button. You will be asked to confirm that you want to add the new threat to the Image Library.

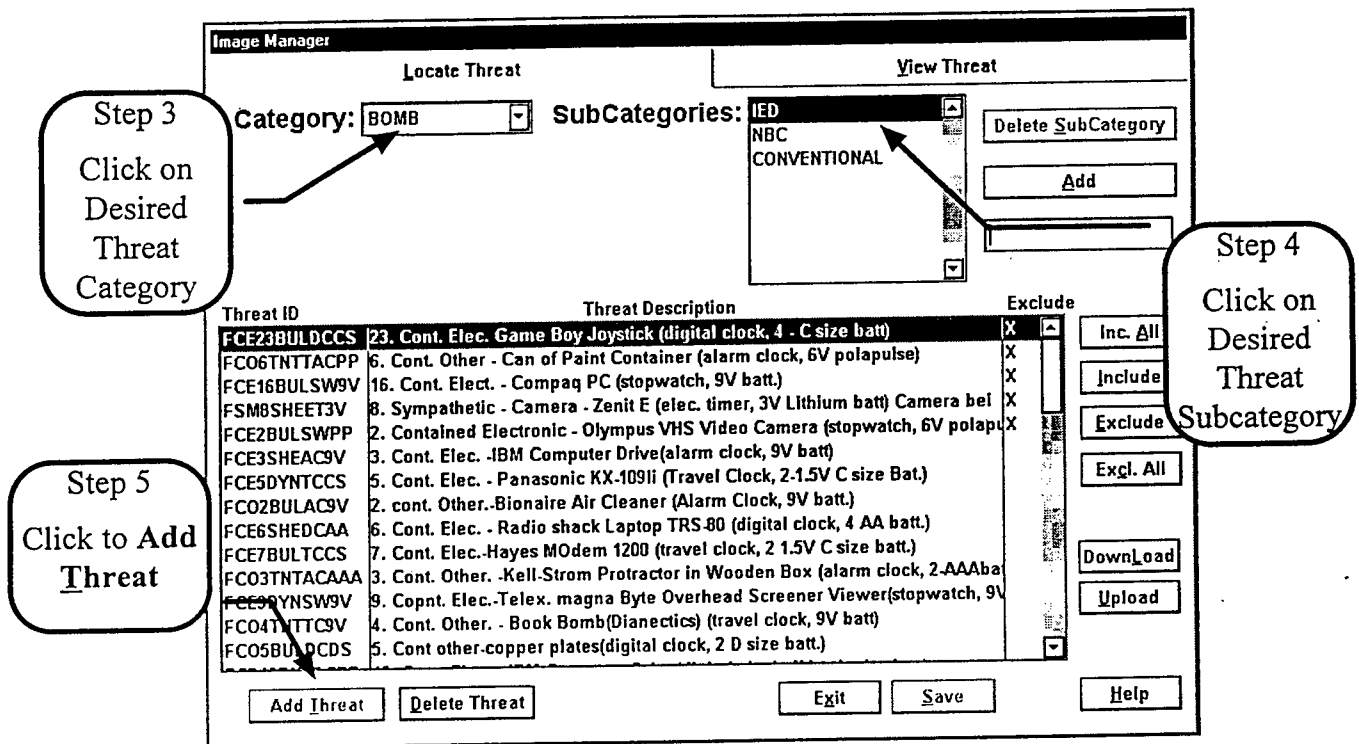


Figure 16b. Adding a new threat image - steps 3, 4, and 5.

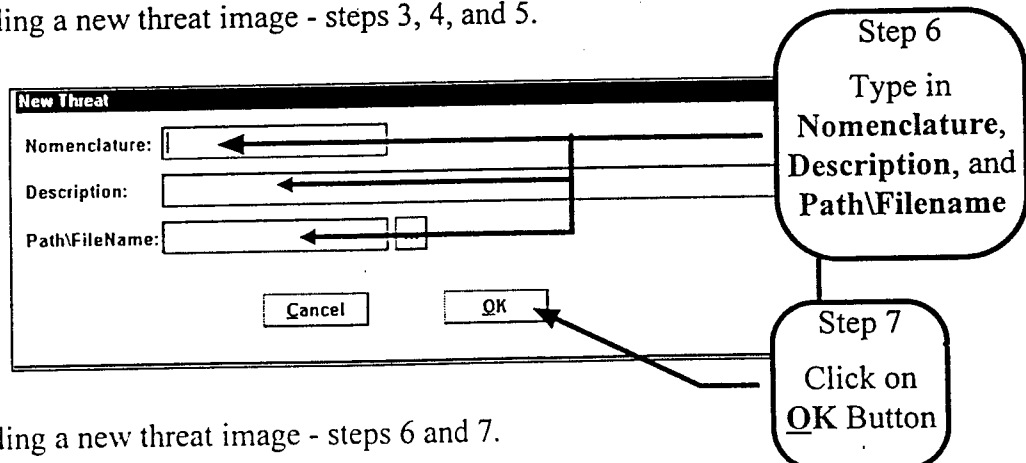


Figure 16c. Adding a new threat image - steps 6 and 7.

How do I download a threat from the Image Library?

(See Figures 17a, 17b, and 17c)

- Step 1. Click on **I**mage **L**ibrary on the menu bar.
- Step 2. Click on **N**avigate/**A**dd/**D**ownload/**U**pload/**D**ele**T**e/**I**nclude/**E**xclude Threats.
- Step 3. Click on the **D**own**L**oad button. (The **S**elect **D**irectory window will appear.)
- Step 4. Click on the down arrow to the right of the **D**rive destination.
- Step 5. Select the **a**: drive (or **d**: for the ZIP drive).
- Step 6. Click on the **S**elect button.

Click on the **Y**es button in the **D**own **L**oad **W**arning box. You will be asked to confirm the downloading sequence.

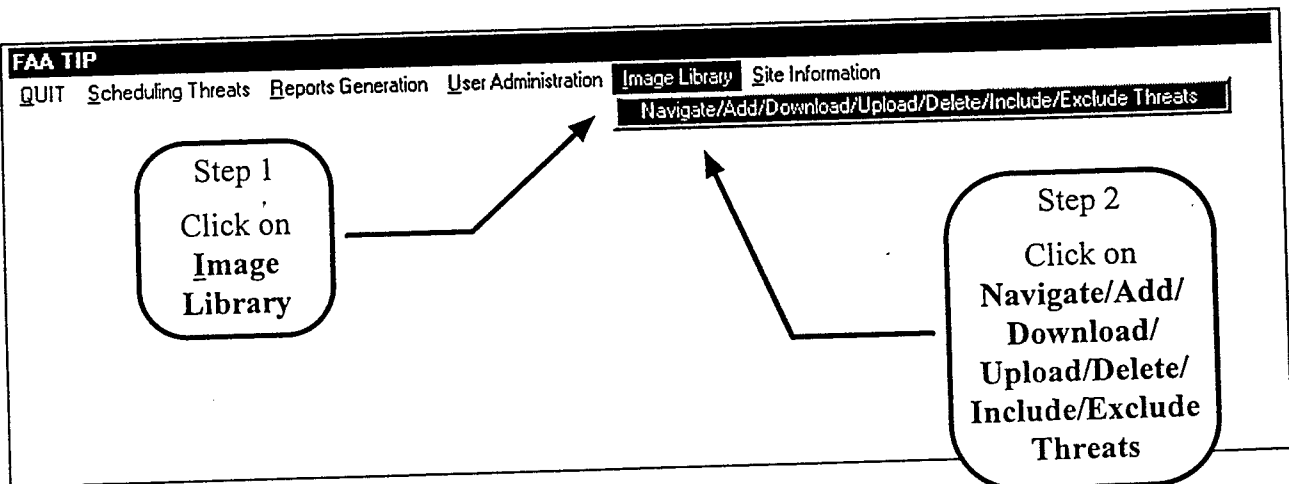


Figure 17a. Downloading a threat from the Image Library - steps 1 and 2.

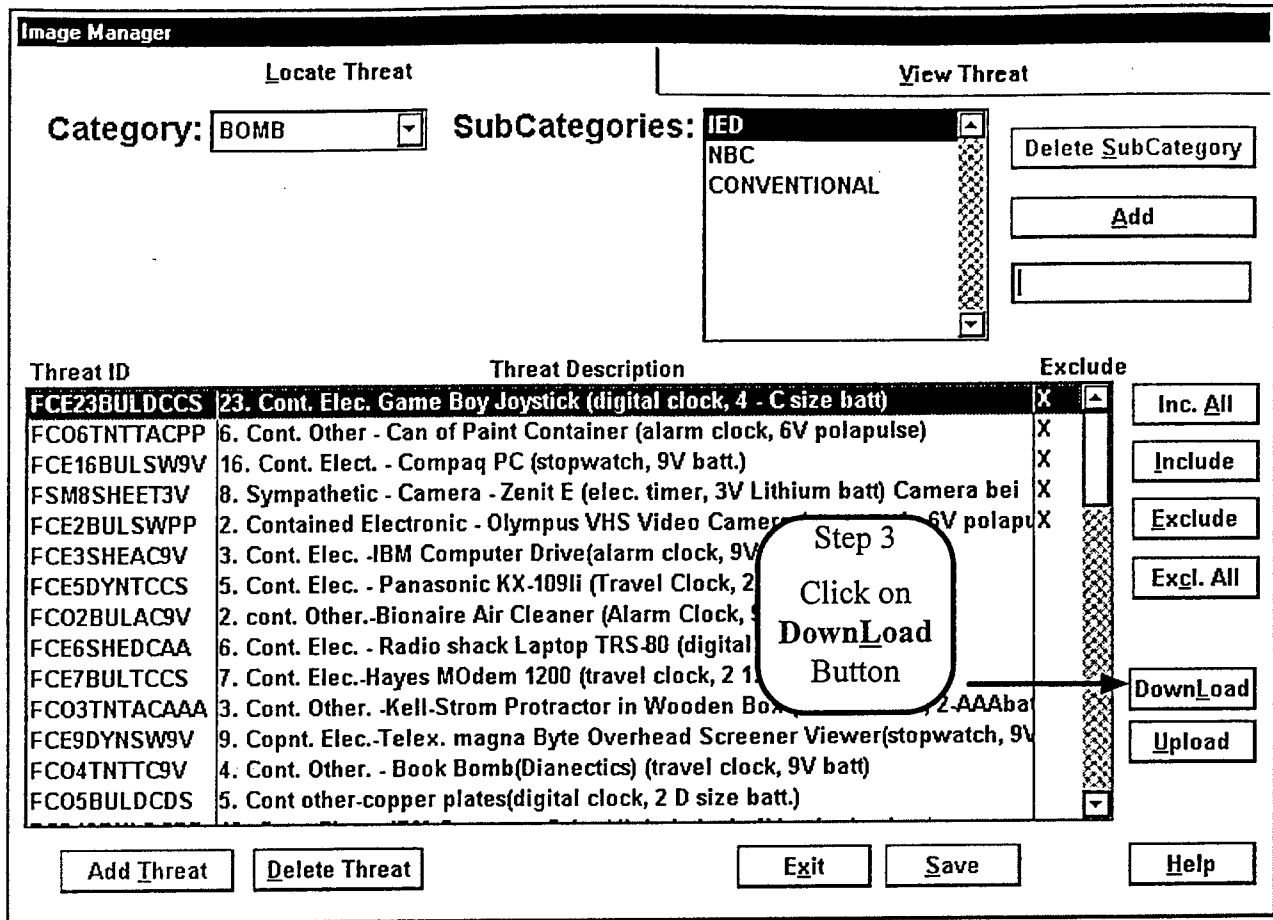


Figure 17b. Downloading a threat from the Image Library - step 3.

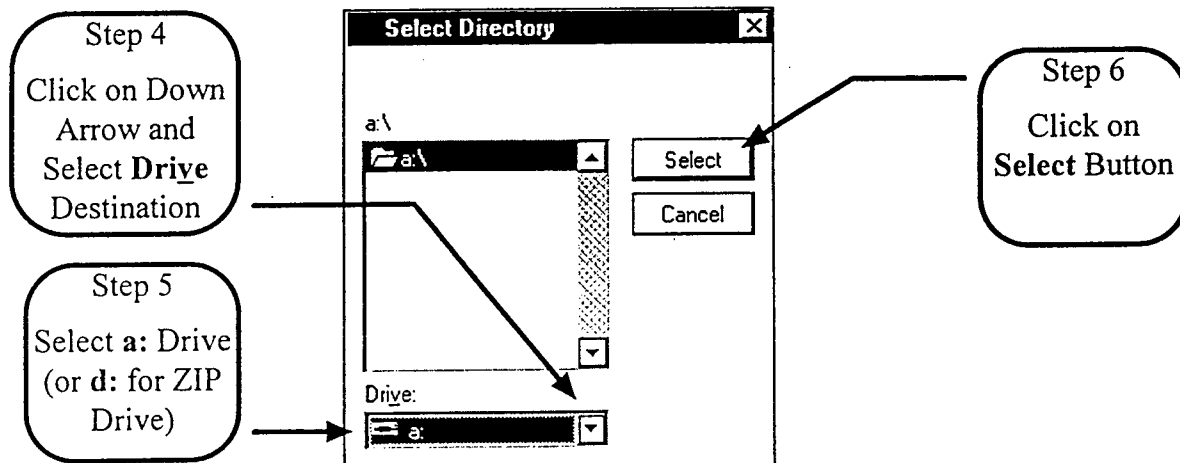


Figure 17c. Downloading a threat from the Image Library - steps 4, 5, and 6.

How do I upload a threat from a disk?

(See Figures 18a, 18b, and 18c)

- Step 1. Click on **I**mage Library on the menu bar.
- Step 2. Click on **N**avigate/**A**dd/**D**ownload/**U**pload/**D**elete/**I**nclude/**E**xclude Threats.
- Step 3. Click on the **U**pload button. (The **O**pen window will appear.)
- Step 4. Click on the down arrow to the right of the **L**ook in box.
- Step 5. Select the A: drive (or D: for the ZIP drive).

After you select the appropriate drive, a list of files will be presented. You will need to double click on the **ThrtDown.DBF** file.

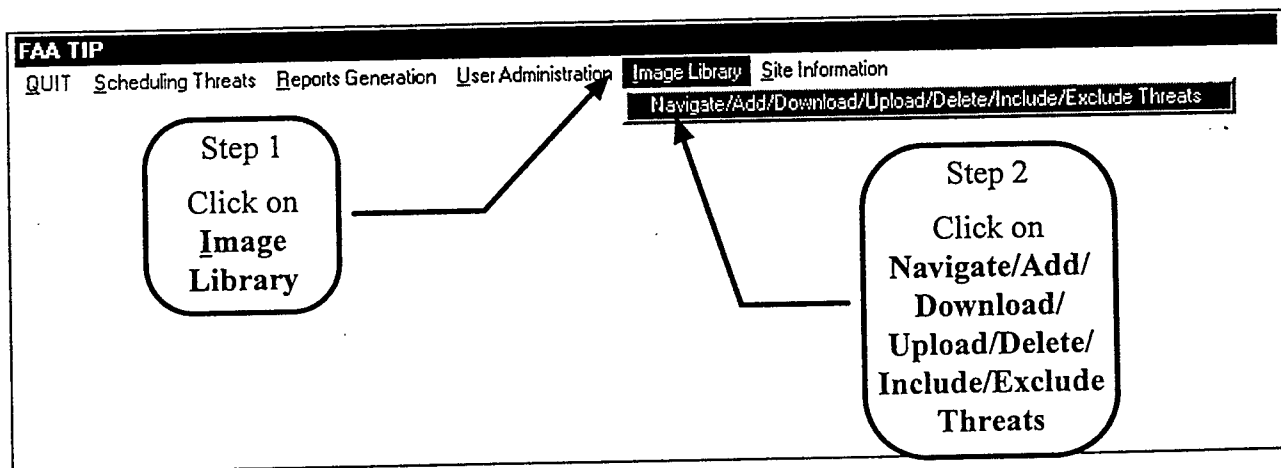


Figure 18a. Uploading a threat from a disk - steps 1 and 2.

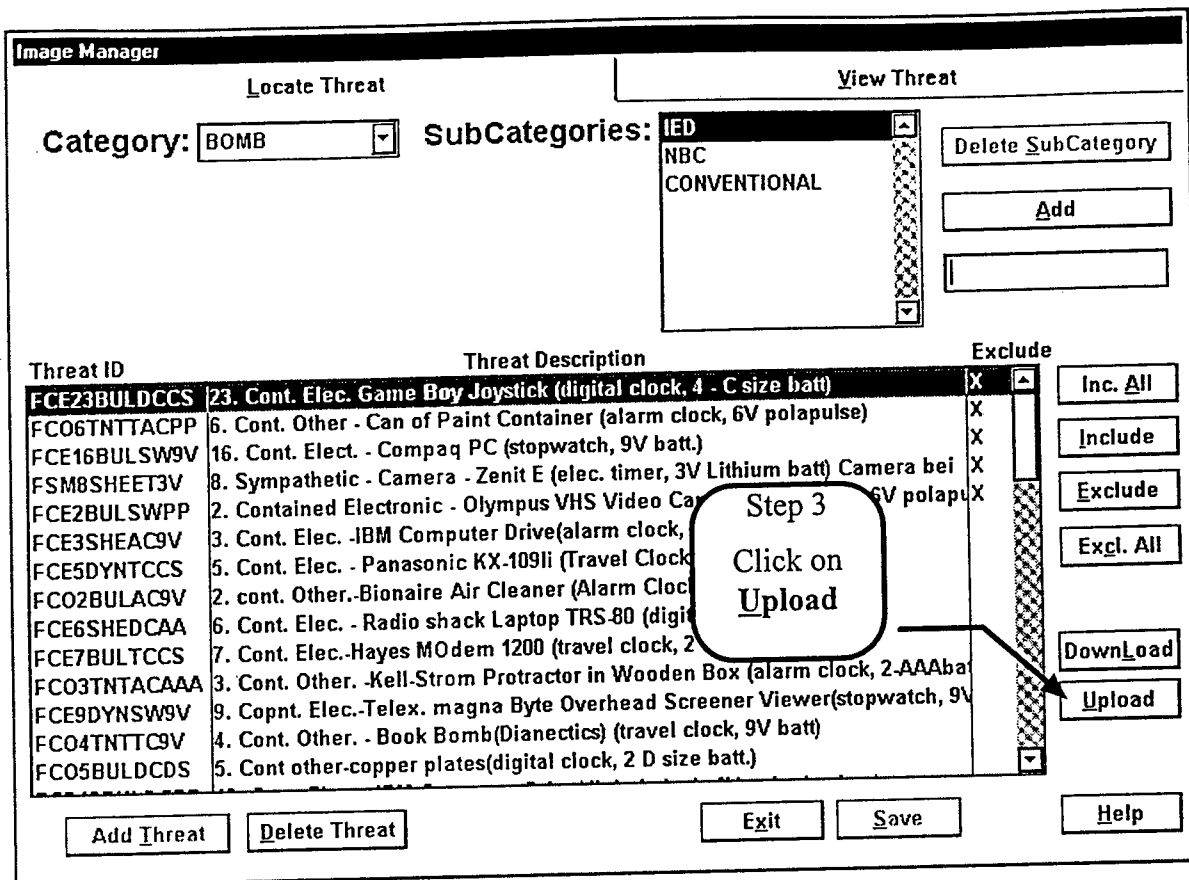


Figure 18b. Uploading a threat from a disk - step 3.

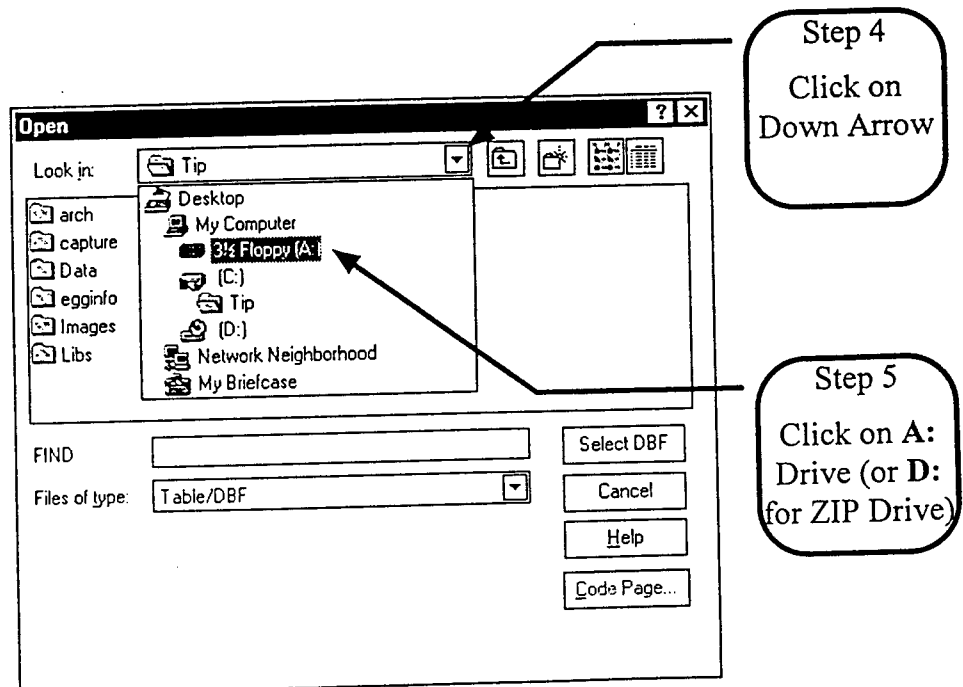


Figure 18c. Uploading a threat from a disk - steps 4 and 5.

How do I delete a threat from the TIP Image Library?

(See Figures 19a and 19b)

Caution: This procedure will permanently delete the selected image from the Threat Image Library. If you just want to exclude the image from the TIP presentation sequence, use the **Exclude** procedures on page 30.

- Step 1. Click on **I**mage Library on the menu bar.

Step 2. Click on **N**avigate/**A**dd/**D**ownload/**U**pload/**D**elete/**I**nclude/**E**xclude Threats.

Step 3. Click on the desired category.

Step 4. Click on the desired subcategory.

Step 5. Click on the threat.

Step 6. Click on the **D**elete Threat button.

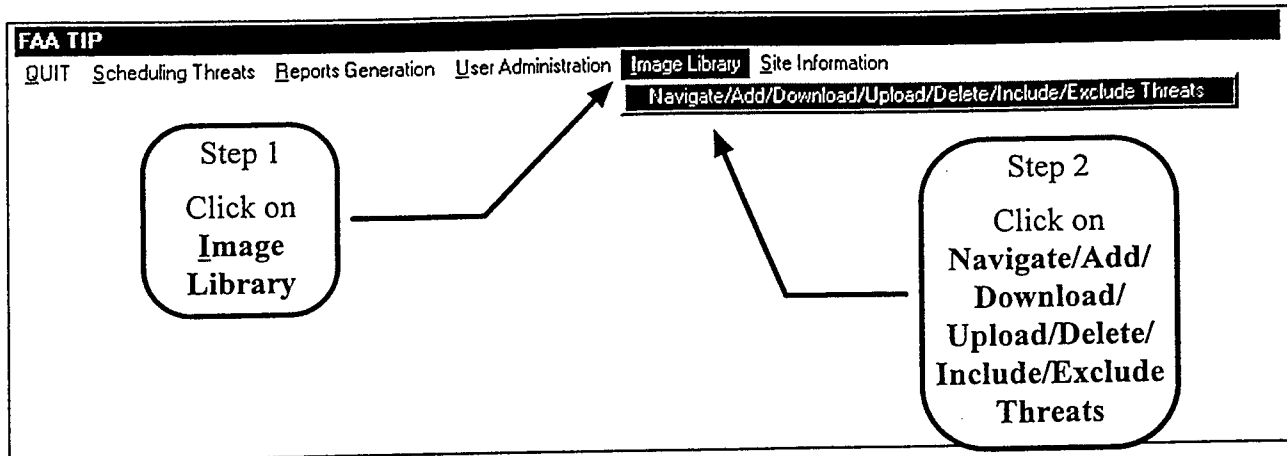


Figure 19a. Deleting a threat from the Threat Image Library - steps 1 and 2.

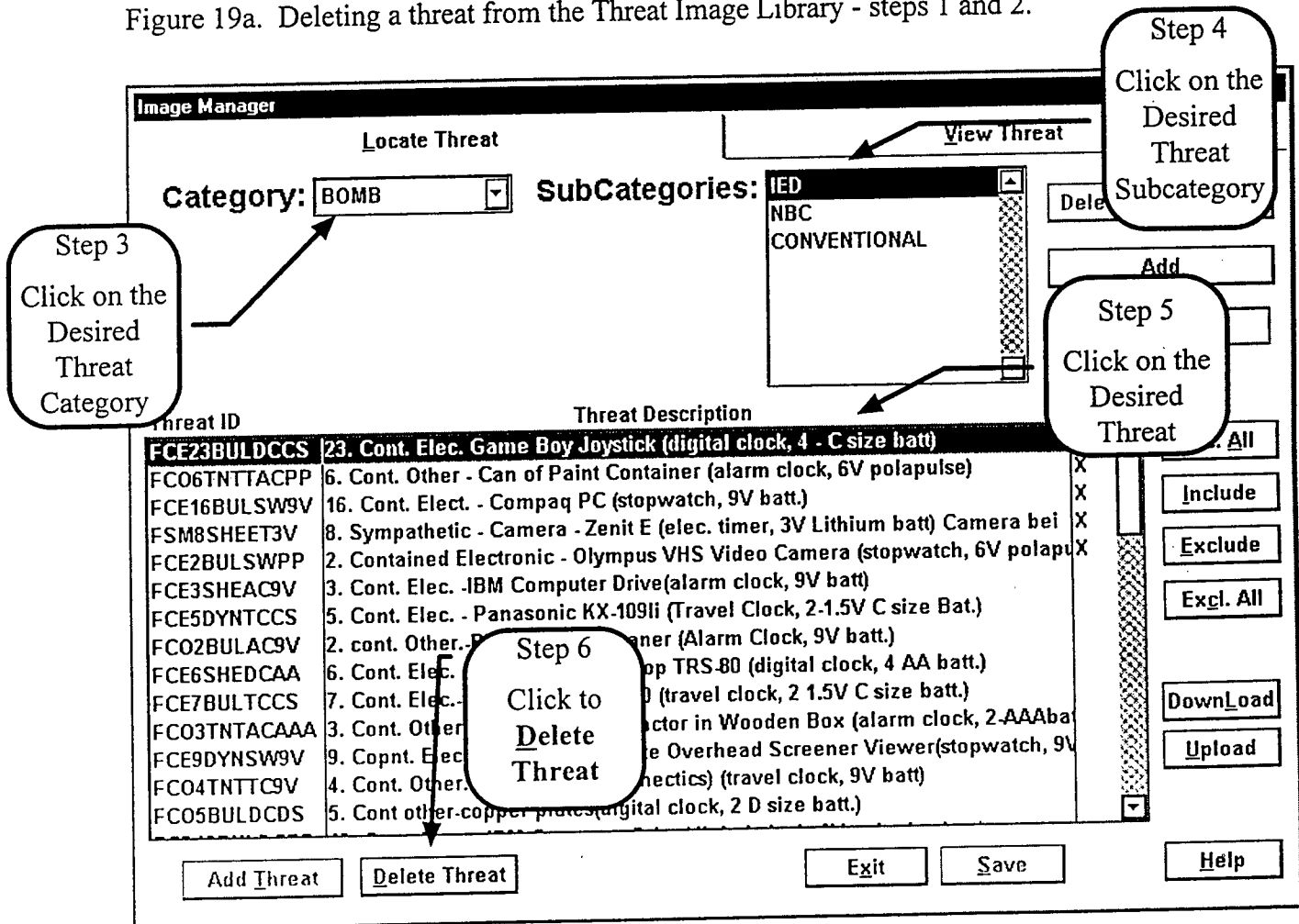


Figure 19b. Deleting a threat from the Threat Image Library - steps 3, 4, 5, and 6.

How do I add a new subcategory?

(See Figures 20a, 20b, and 20c)

- Step 1. Click on **I**mage Library on the menu bar.
- Step 2. Click on **N**avigate/**A**dd/**D**ownload/**U**pload/**D**elete/**I**nclude/**E**xclude Threats.
- Step 3. Click on the **N**ew SubCategory button. (The **N**ew SubCategory button will change to an **A**dd button, and a text box will appear below it.)
- Step 4. Type in the new threat subcategory.
- Step 5. Click on the **A**dd button.
- Step 6. Click on the **S**ave button.

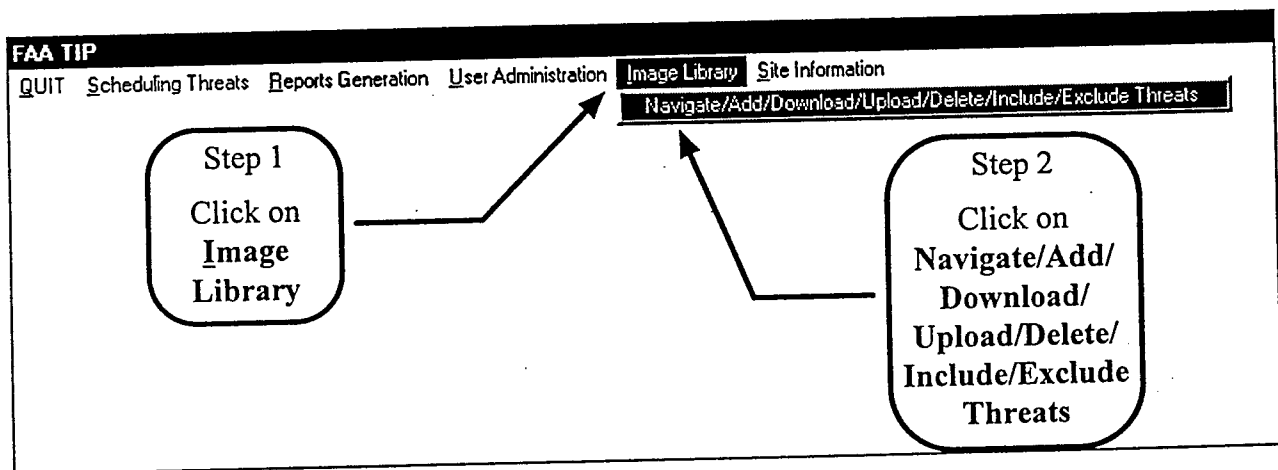


Figure 20a. Adding a new threat subcategory - steps 1 and 2.

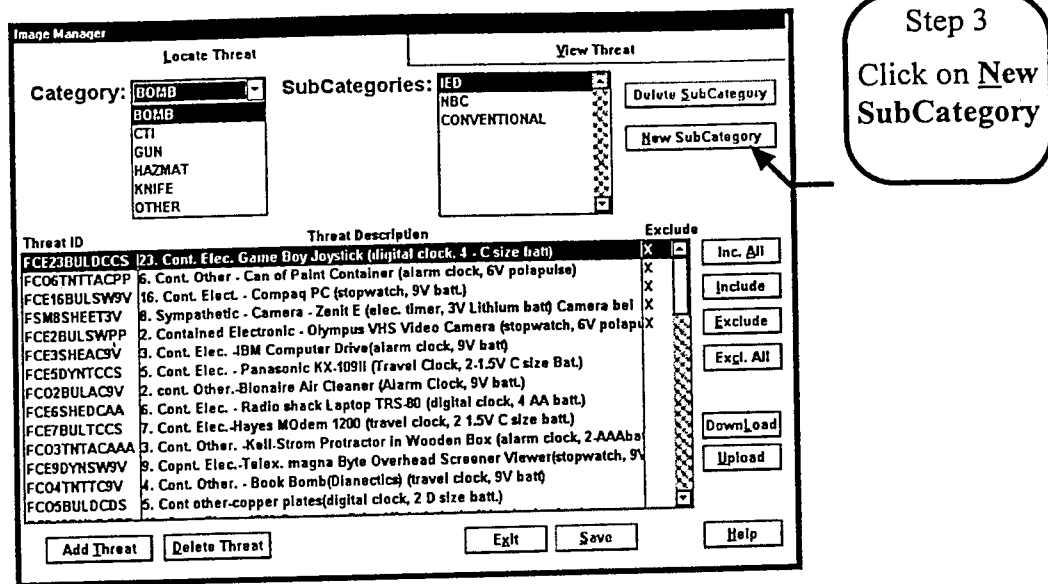


Figure 20b. Adding a new threat subcategory - step 3.

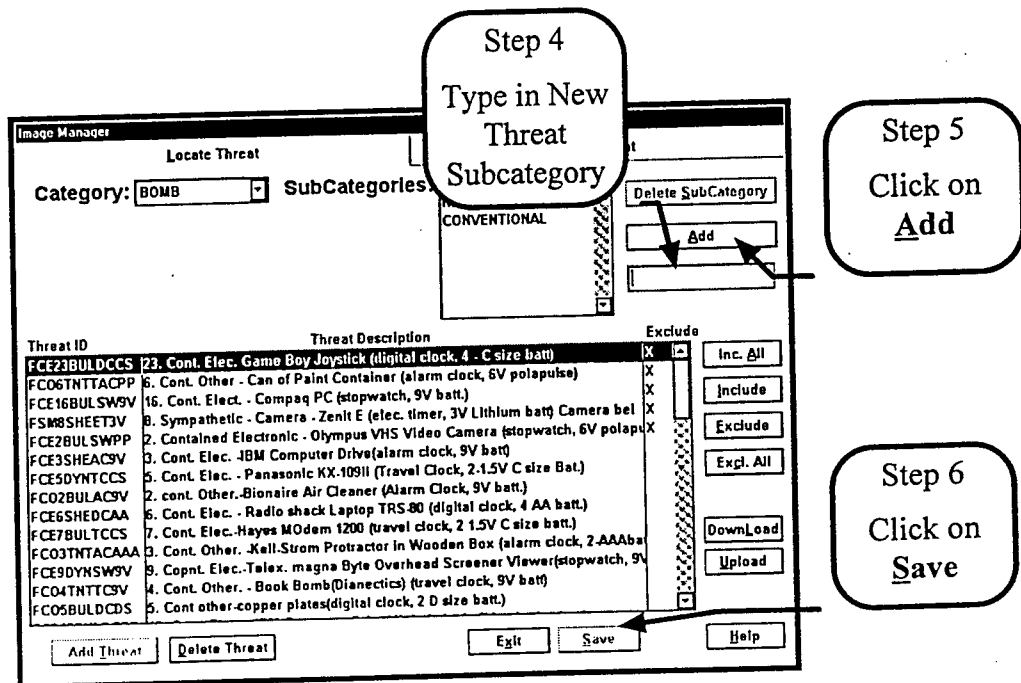


Figure 20c. Adding a new threat subcategory - steps 4, 5, and 6.

Management of the Threat Image Presentation Schedule

What is the threat image presentation schedule?

The presentation of threats is controlled by the TIP scheduling function and it determines how frequently threat images appear. It also regulates ratios of presentations within categories (e.g., bombs, guns, knives) and subcategories (e.g., bombs - improvised explosive device) of threats. For example, the relative ratios could be set at 40% bombs, 35% guns, and 25% knives. The only restriction is that the percentages of all categories and subcategories must total 100%.

The frequency of the various presentations can be changed only by FSMs and selected FAA personnel.

What topics will be covered in this section?

1. Setting threat presentation frequency ratios
2. Setting percentages of threats to be presented

How does the schedule work?

Setting threat presentation frequency ratios

- ⇒ Bag ratio - Determines the average number of bags that are presented before a TIP image is presented.
- ⇒ Variance - Determines the range between the minimum and maximum number of bags that will be screened before the next TIP image is presented.

The bag ratio minus the variance equals minimum number of bags screened before a TIP image is presented.

The bag ratio plus the variance equals maximum number of bags screened before the next TIP image is presented.

- ⇒ Random ratio - Sets the percentage of TIP images that are presented randomly.
- ⇒ Random bag ratio - Sets the range of bags in which a TIP image is randomly presented.

Setting percentages of threats to be presented

- ⇒ Percentages - Sets the percentage of threat categories and subcategories to be presented.

How do I set threat presentation frequency ratios?

(See Figures 21a and 21b)

- Step 1. Click on **S**cheduling Threats on the menu bar.

Step 2. Click on **F**requency Ratios.

Step 3. Click on the arrows next to the **B**ag Ratio box to increase or decrease the number of bags that will pass before a TIP is presented.

Step 4. Click on the arrows next to the **V**ariance box to increase or decrease the variance in the TIP presentation sequence.

Step 5. Click on the arrows next to the **R**andom Ratio box to increase or decrease the percentage of TIP images that will be presented randomly.

Step 6. Click on the arrows next to the **R**andom Bag Ratio boxes to increase or decrease the random range.

Step 7. Click on the **O**K button to save changes.

OR

Click on the **C**ancel button to abandon changes.

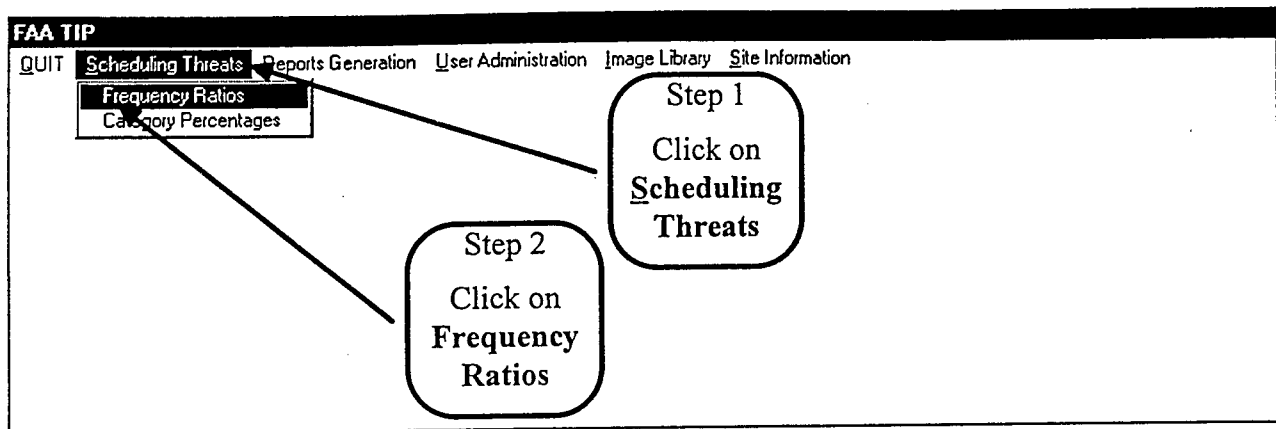


Figure 21a. Setting TIP presentation frequency ratios - steps 1 and 2.

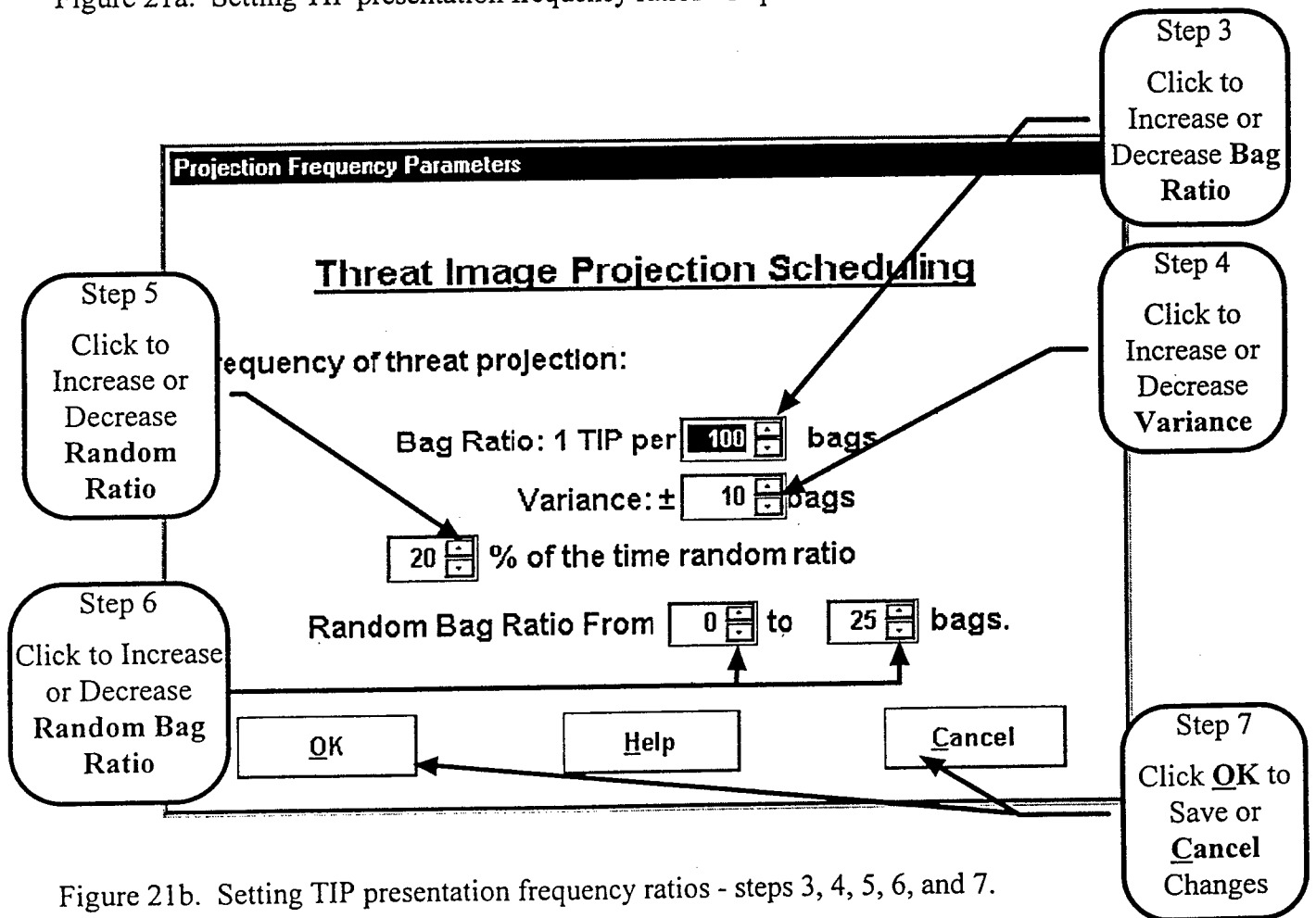


Figure 21b. Setting TIP presentation frequency ratios - steps 3, 4, 5, 6, and 7.

How do I set the percentages of threats to be presented?

(See Figures 22a and 22b)

Step 1. Click on **S**cheduling Threats on the menu bar.

Step 2. Click on **C**ategory Percentages.

Step 3. Click on the % column entry for each threat subcategory to be changed.
Type in the new percentage values.

Note: The sum of threat subcategory percentages must total 100%.

Step 4. Click on the **O**K button to save changes.

OR

Click on the **C**ancel button to abandon changes.

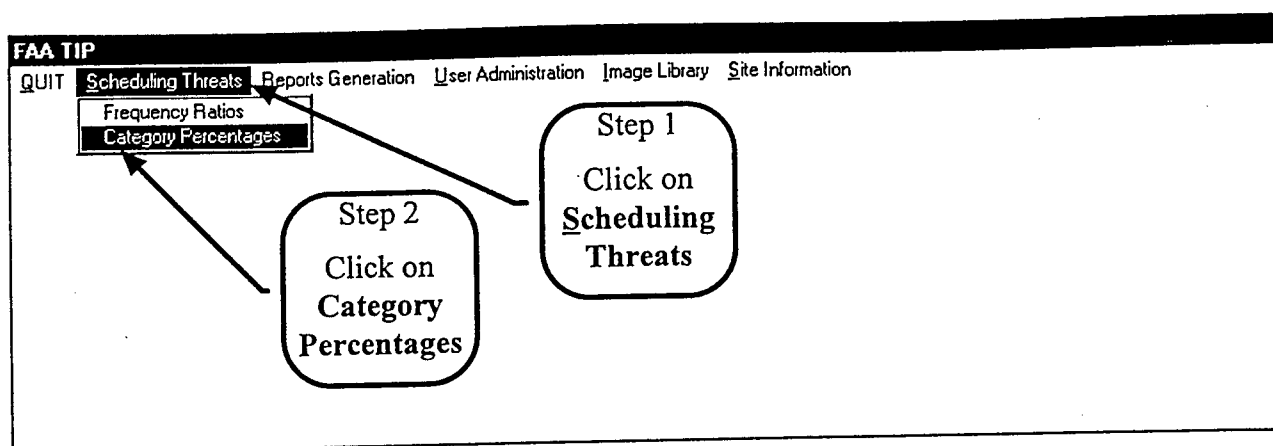


Figure 22a. Setting category and subcategory percentages - steps 1 and 2.

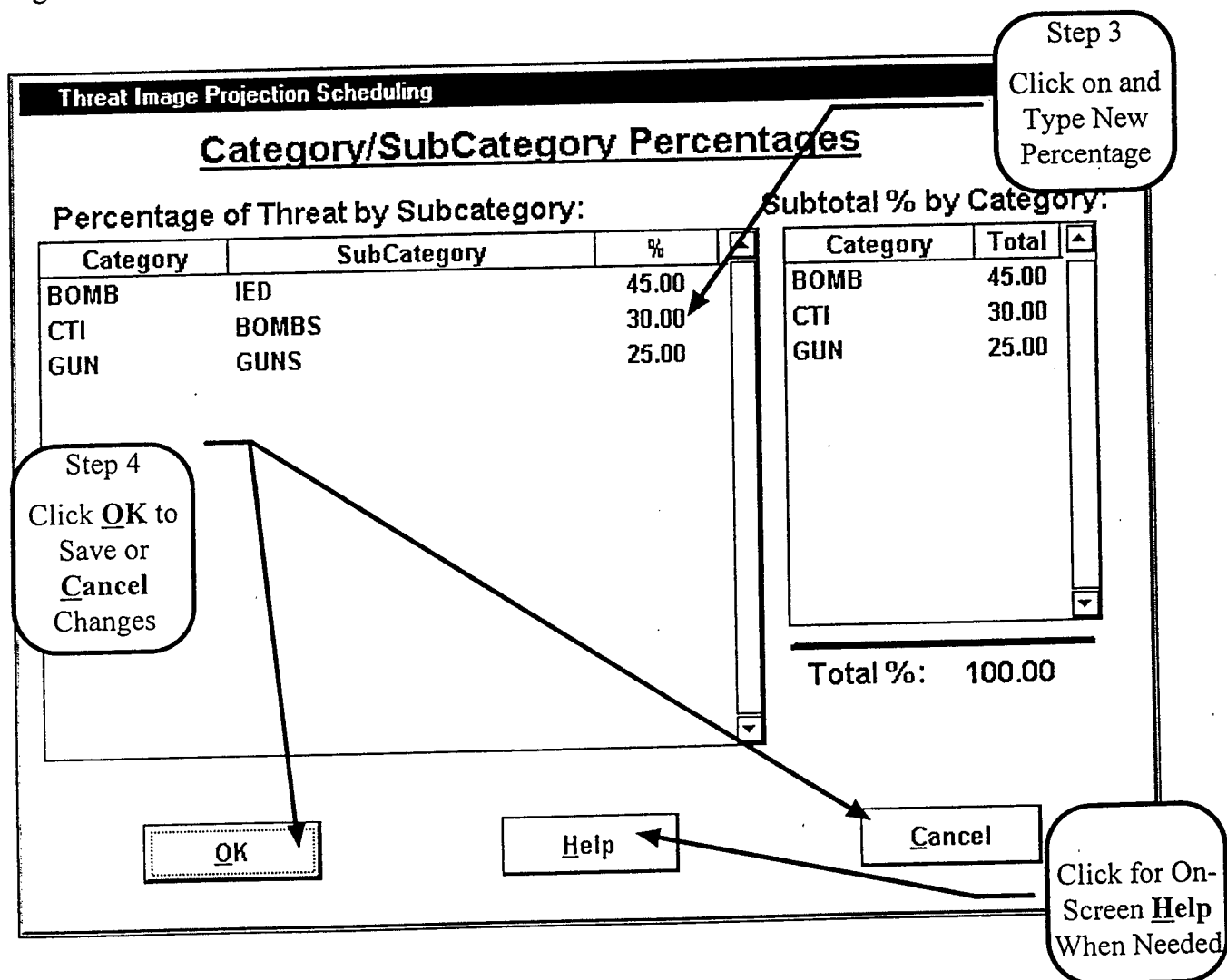


Figure 22b. Setting category and subcategory percentages - steps 3 and 4.

Downloading Monthly Data Reports

What is involved?

There are four reports that need to be downloaded to create a complete TIP data set. They are as follows

1. Screener Log
2. Individual Screener Performance Report
3. Screener Comparisons Report
4. Threat Image Projection Details Report

The FAA requires that all four reports be downloaded and submitted every month during the demonstration testing period.

Caution: If TIP reports have not been downloaded for 3 consecutive months, the machine will shut down. Downloading all four reports for each month will automatically restart the machine.

How do I download the Screener Log Report?

Note: Before beginning the report download sequence, you must insert a disk into drive "A" or the "D" drive for ZIP disks. The disk should remain in the drive until all four reports have been downloaded.

(See Figures 23a and 23b)

Step 1. Click on **Reports Generation** from the menu bar.

Step 2. Click on **Screener Log**.

Step 3. Click on the desired month/year.

Step 4. Click on the **Down Load** button.

Step 5. Click on the **Exit** button.

This concludes the Screener Log download procedure. You are now ready to download the Individual Screener Performance Report.

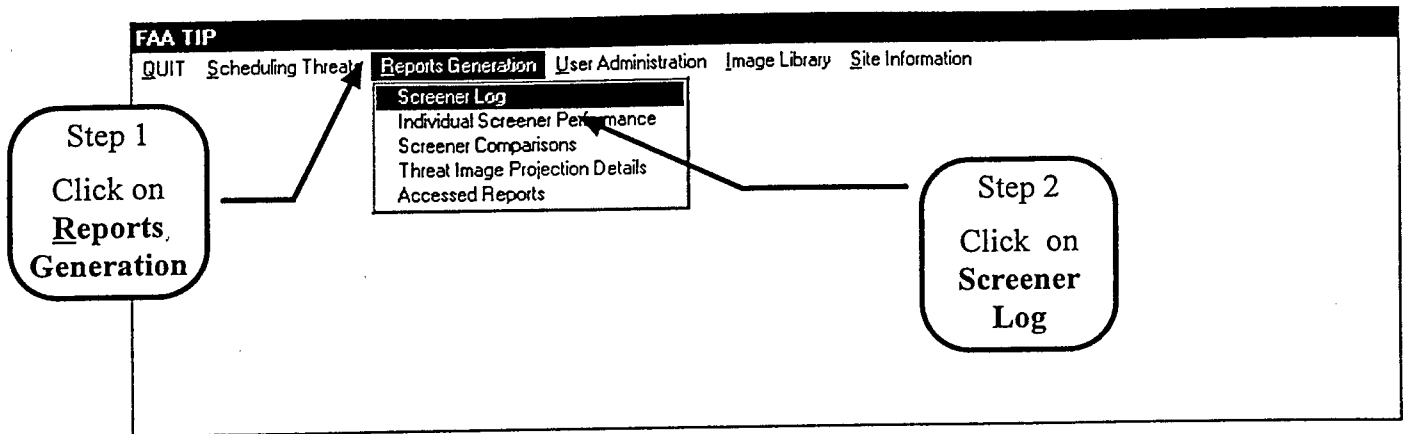


Figure 23a. Downloading the Screener Log report - steps 1 and 2.

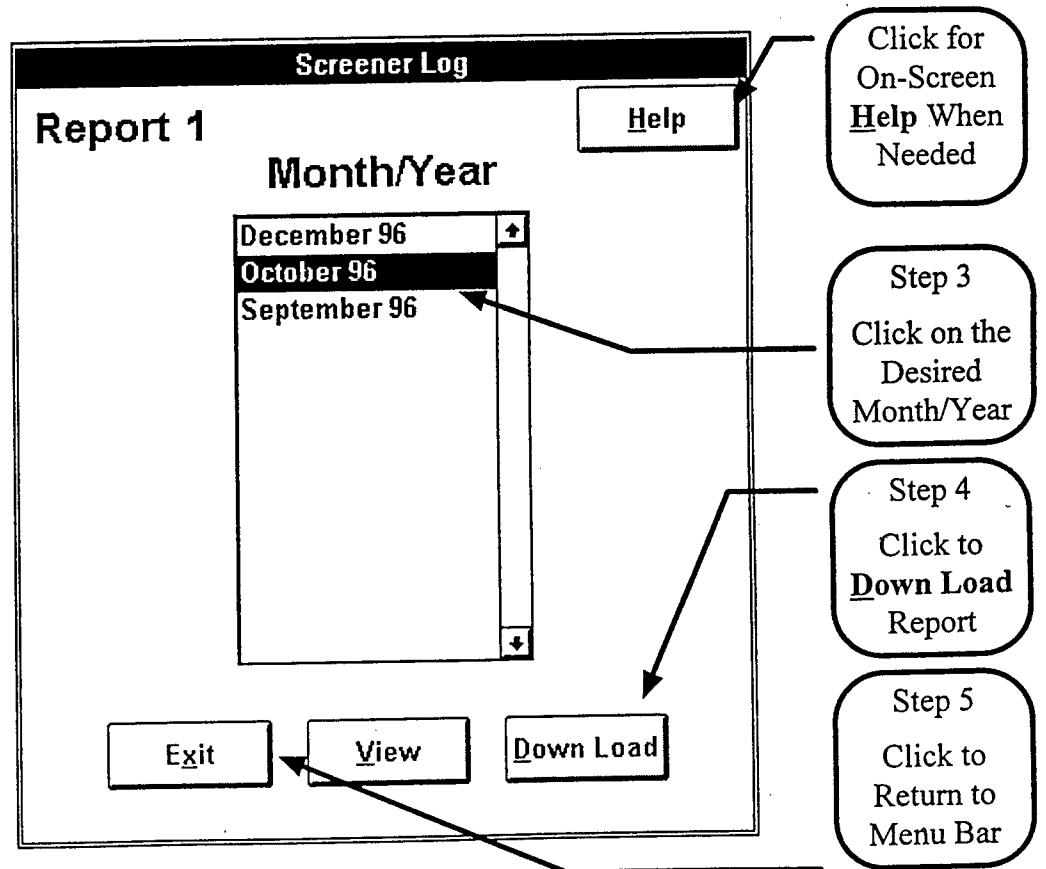


Figure 23b. Downloading the Screener Log report - steps 3, 4, and 5.

How do I download the Individual Screener Performance Report?

Note: This is a continuation of report downloading procedures. See page 52 for the beginning of the report download procedures.

(See Figures 24a and 24b)

Step 1. Click on **Reports Generation** from the menu bar.

Step 2. Click on **Individual Screener Performance**.

Step 3. Click on the **Down Load All Screeners** button.

Step 4. Click on the **Exit** button.

This concludes the Individual Screener Performance Report download. You are now ready to download the Screener Comparisons Report.

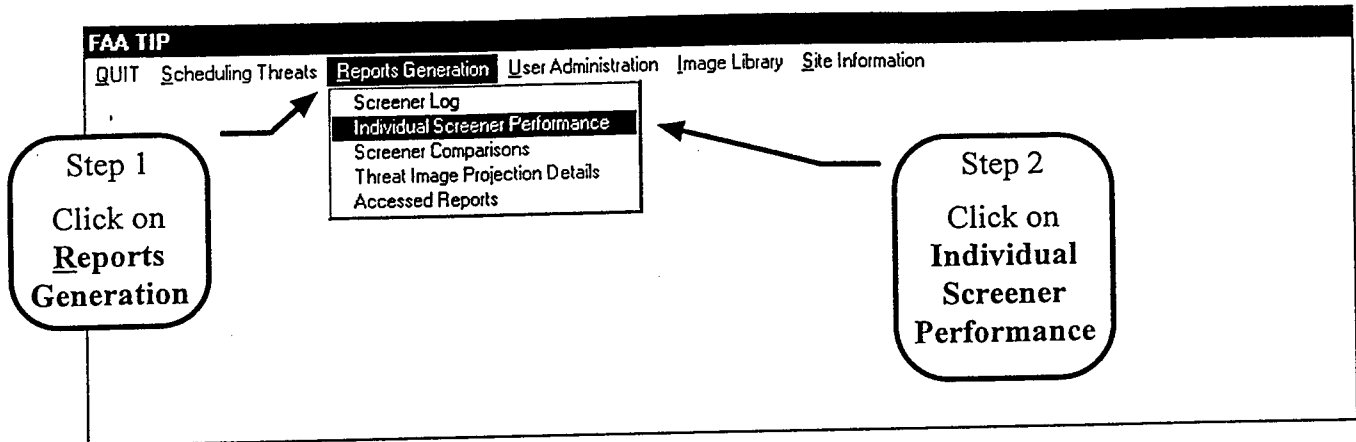


Figure 24a. Downloading the Individual Screener Performance report - steps 1 and 2.

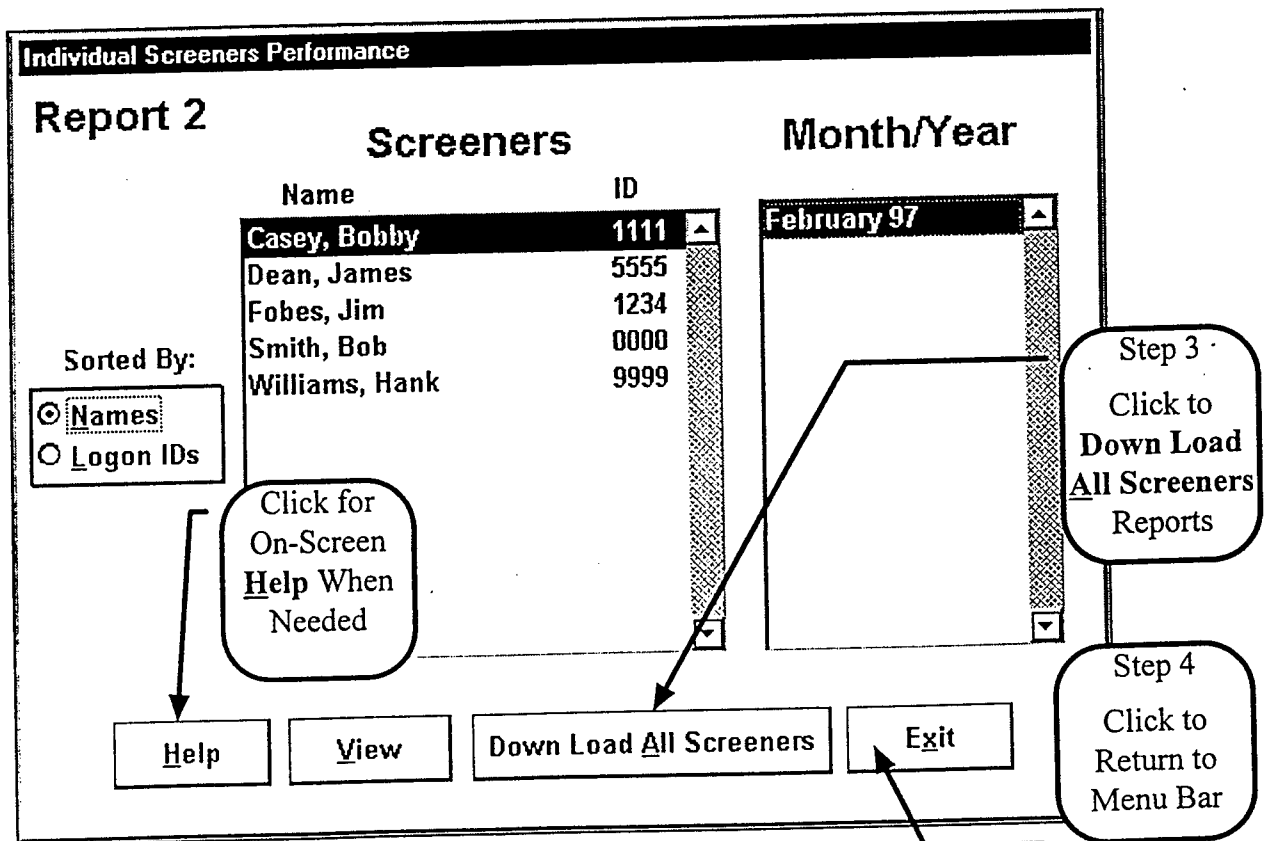


Figure 24b. Downloading the Individual Screener Performance report - steps 3, and 4.

How do I download the Screener Comparisons Report?

Note: This is a continuation of report downloading procedures. See page 52 for the beginning of the report download procedures.

(See Figures 25a and 25b)

Step 1. Click on **Reports Generation** from the menu bar.

Step 2. Click on **Screener Comparisons**.

Step 3. Click on the desired month/year.

Step 4. Click on the **Down Load** button.

Step 5. Click on the **Exit** button.

This concludes the Screener Comparisons Report download procedure. You are now ready to download the Threat Image Projection Details Report.

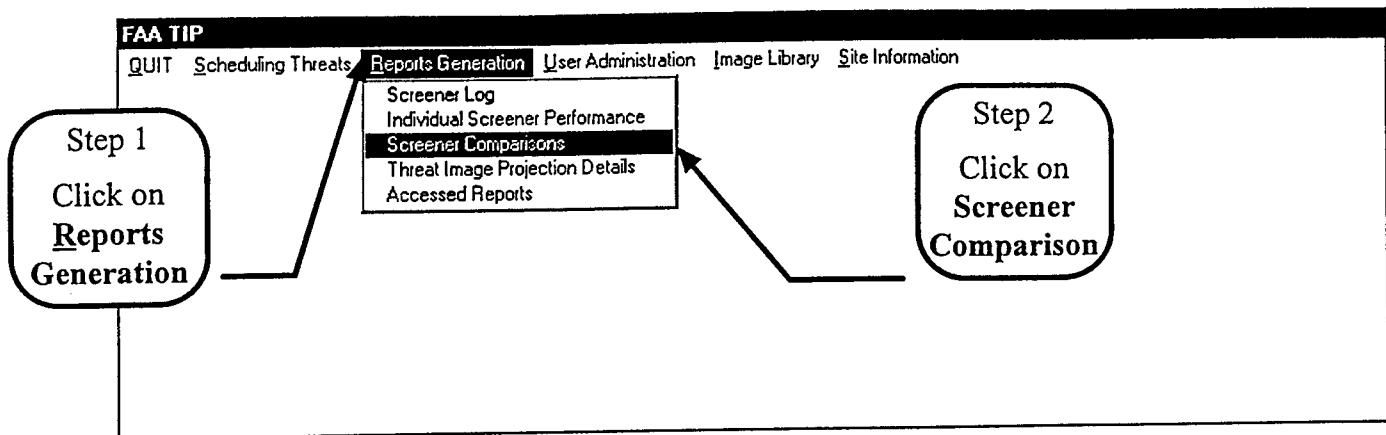


Figure 25a. Downloading the Screener Comparisons report - steps 1 and 2.

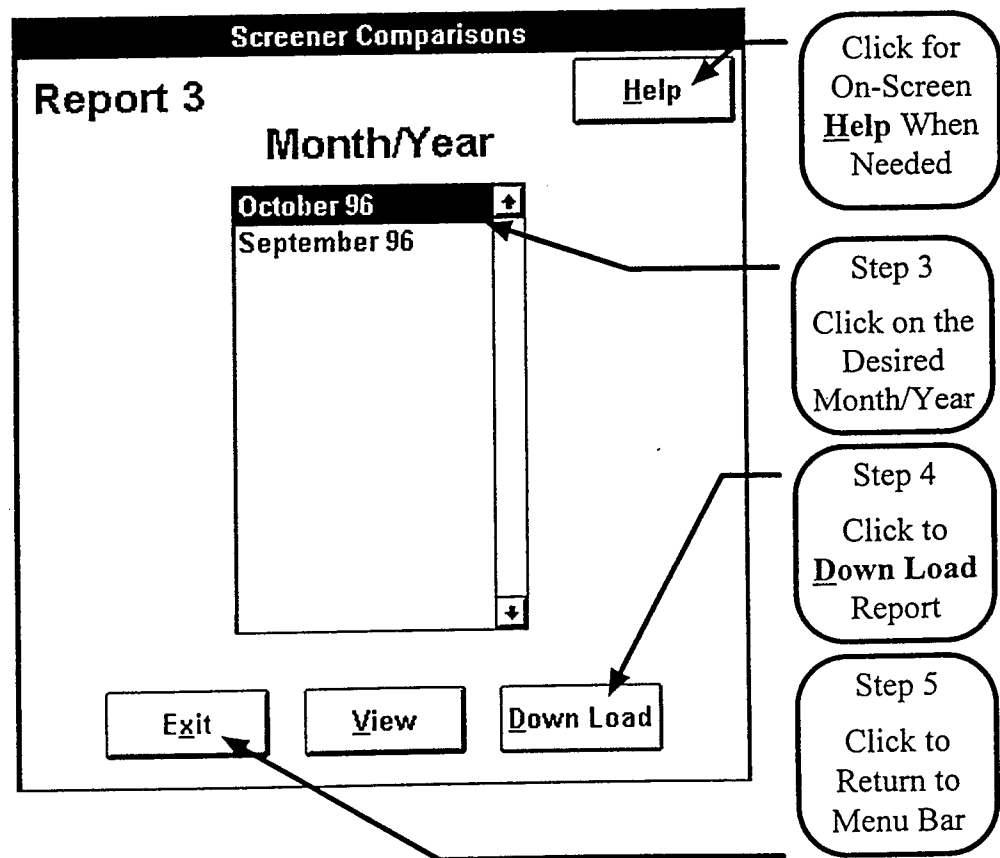


Figure 25b. Downloading the Screener Comparisons report - steps 3, 4, and 5.

How do I download the Threat Image Projection Details Report?

Note: This is a continuation of the report downloading procedures. See page 52 for the beginning of the report downloading procedures.

(See Figures 26a and 26b)

Step 1. Click on **Reports Generation** from the menu bar.

Step 2. Click on **Threat Image Projection Details**.

Step 3. Click on the desired month/year.

Step 4. Click on the **Down Load** button.

Step 5. Click on the **Exit** button.

This concludes the report downloading procedures.

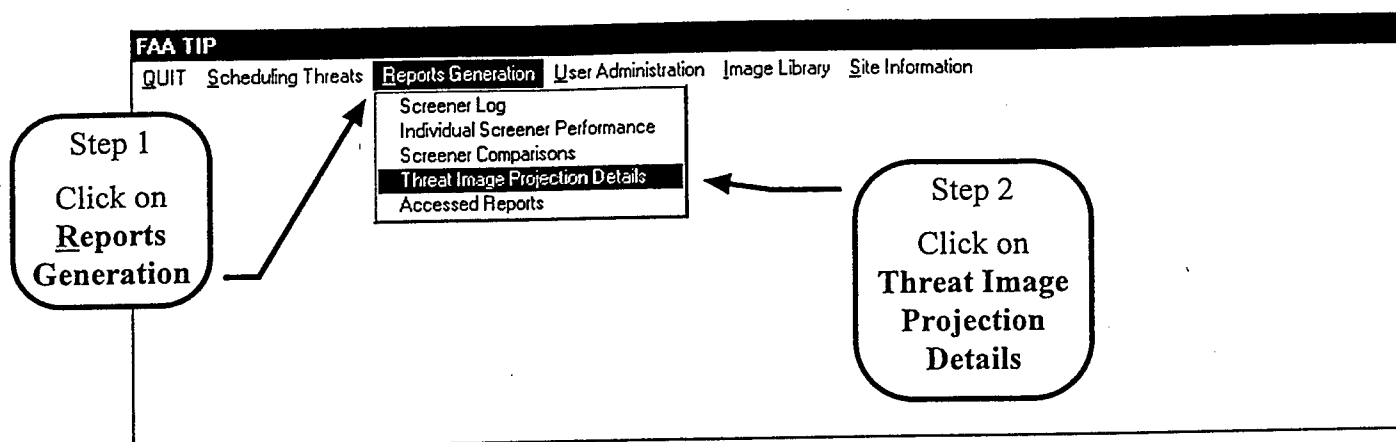


Figure 26a. Downloading the Threat Image Projection Details report - steps 1 and 2.

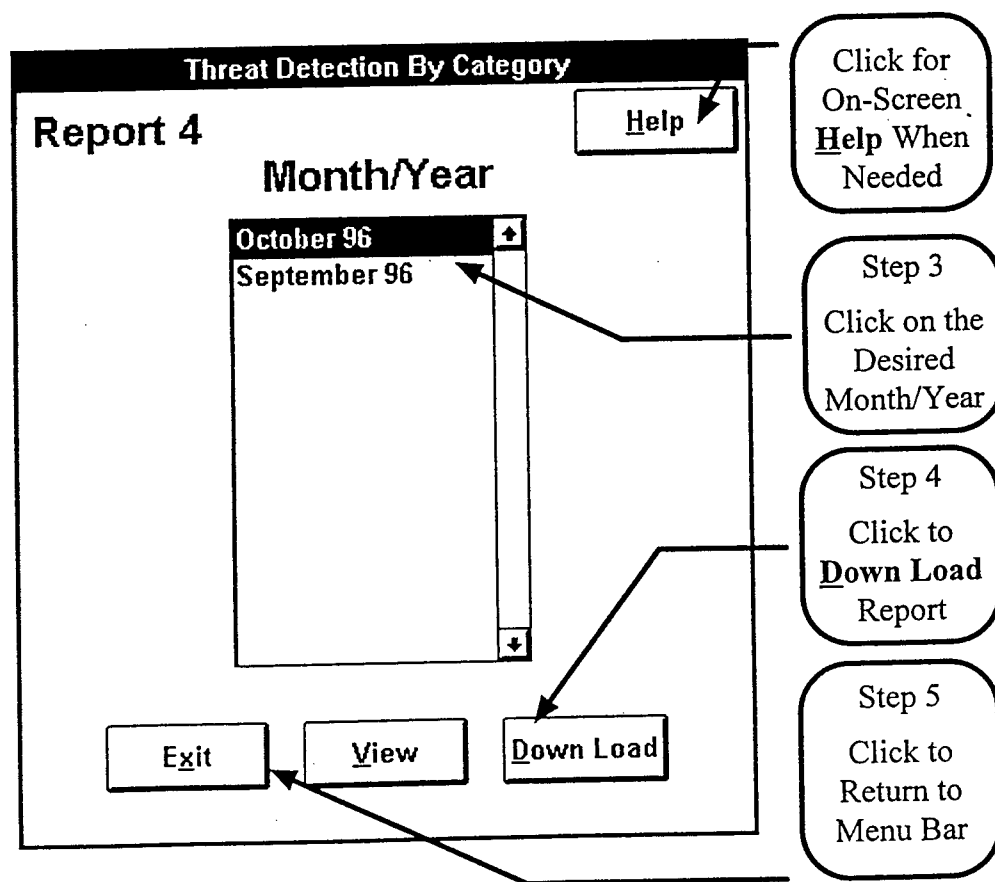


Figure 26b. Downloading the Threat Image Projection Details report - steps 3, 4, and 5.

Where do I send the monthly data disks?

The FSM will receive a pre-addressed envelope each month when they receive their disk.

The address is:

FAA William J. Hughes Technical Center
Aviation Security Human Factors Program
Attention: Brenda A. Klock, AAR-510
Building 315
Atlantic City International Airport, NJ 08405

EG&G Astrophysics
Threat Image Projection
Checkpoint Security Supervisors' Guide



User Guide II

Table of Contents

	Page
Threat Image Projection System: Overview for EG&G X-Ray Machines	1
What is Threat Image Projection (TIP)?	1
What does TIP do?	1
How does TIP work?	1
What is the purpose of this training?	1
What will this guide tell me?	1
Log In	2
Who can log in?	2
How do I log in?	2
Security Access Levels	4
How is access to TIP functions and reports controlled?	4
Who will be able to do what?	4
Report Overviews	5
What reports are available?	5
How does TIP generate these reports?	5
Screener Log Report: Overview and Generation	6
What is a Screener Log Report?	6
What does each column heading mean?	6
How do I view a Screener Log Report?	8
Individual Screener Performance Summary Comparisons Report: Overview and Generation	10
What is a Screener Performance Report?	10
What does each column heading mean?	10
How do I view an Individual Screener Performance Report?	12
Screener Comparisons Report: Overview and Generation	14
What is a Screener Comparisons Report?	14
What does each column heading mean?	14
How do I get a Screener Comparisons Report?	16
Threat Image Projection Details Report: Overview and Generation	18
What is a Threat Image Projection Details Report?	18
What does each column heading mean?	18
How do I get a Threat Image Projections Details Report?	20
Log Out	22
How do I log out?	22

Threat Image Projection System: Overview for EG&G X-Ray Machines

What is Threat Image Projection (TIP)?

TIP is a modification of the X-ray system that allows images of threats (e.g., guns, knives, bombs, and hazardous materials) to be included in the displayed image of passenger bags. The TIP system is being installed at airport baggage checkpoints across the country.

What does TIP do?

TIP is designed to teach screeners about a variety of threats. TIP provides the screeners with experience in recognizing threats as they would appear in actual passenger baggage.

TIP is expected to increase awareness and recognition of threats by screeners and supervisors. In addition to providing screeners with practice in recognizing threats, TIP keeps a record of the threats correctly identified by screeners and those missed. To improve training, screener performance is tracked by supervisors, airport security staff, and Federal Aviation Administration (FAA) personnel.

How does TIP work?

TIP projects X-ray images of threats onto actual passenger bags and bags that are not really there (fictional bags) during the normal passenger baggage screening process. The screener pushes the **Threat** button on the console when they detect a threat. TIP provides on-screen feedback when the threat is a projected image.

Important Reminder: Screeners should be frequently reminded to push the **Threat** button whenever they see a threat on their baggage X-ray computer screen. The TIP system will provide on-screen feedback to the screener if the threat is a projected image and the threat image will clear. If the image does not clear after pushing the **Threat** button, screeners should follow airport procedures for actual threats.

What is the purpose of this training?

A half-hour training session is offered to accompany this handbook and the installation of TIP. It is provided by the FAA to introduce TIP system operation and interpretation of TIP reports to Federal Security Managers, Station Managers, Security Company Managers, and Checkpoint Security Supervisors (CSSs).

What will this guide tell me?

This handbook is designed to help you navigate through TIP system operations and to help you understand the reports it generates.

Log In

Who can log in?

Everyone with a user ID number and password will be able to log in to the TIP system.

How do I log in?

To log in, follow the procedures below and refer to Figure 1.

- Step 1. Click on the text box next to **USER ID:** and type your user ID number.
- Step 2. Click on the text box next to **PassWord:** and type your password.
- Step 3. Click on the **OK** button. (or press the **Enter** key on keyboard).

Note: Ensure that screeners log in using their own passwords. Passwords should be kept confidential. CSSs will be able to monitor who is logged in. The screener's name will be displayed in the lower right hand corner of the screen.

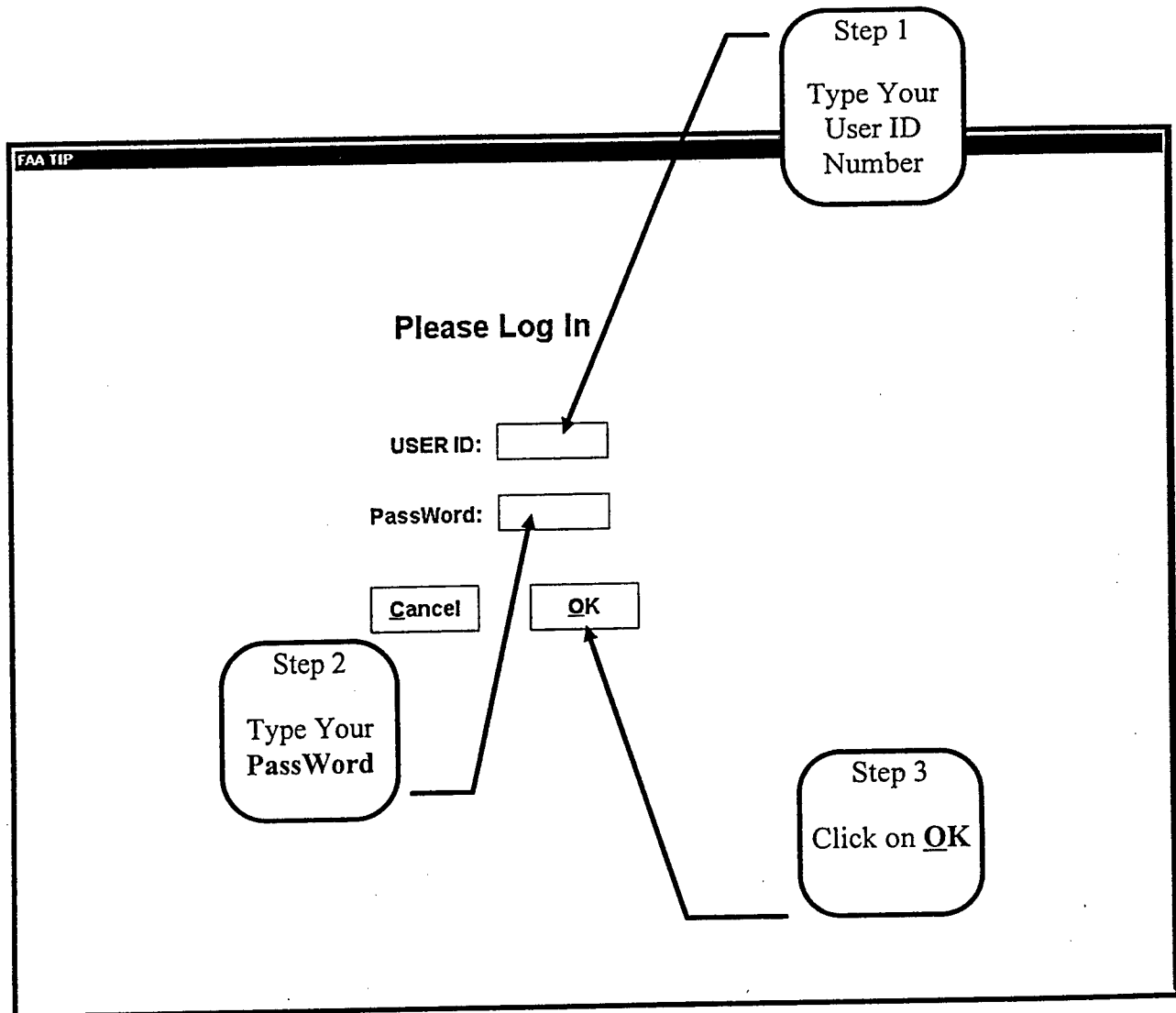


Figure 1. Log in procedure - steps 1, 2, and 3.

Security Access Levels

How is access to TIP functions and reports controlled?

There are multiple Security Access Levels depending on the user's needs. This guide pertains only to levels for CSSs and screeners. The log in sequence and password tell the computer the access level of each user.

Who will be able to do what?

Table 1 shows who may access different functions and reports generated by the TIP system. The user's security access level allows them to perform the functions within their cell and below (e.g., CSSs can log in and log out of the system as well as view TIP reports).

Table 1. TIP User Levels and Functions

User	Functions
Checkpoint Security Supervisor (CSS)	View TIP Reports
Screener	Log in Log out

Note: Screeners will only be able to log in and log out of the machine to screen bags. They will not have access to any reports or information.

Report Overviews

What reports are available?

The four TIP reports are listed below:

1. Screener Log
2. Individual Screener Performance Summary Comparisons
3. Screener Comparisons
4. Threat Image Projection Details

How does TIP generate these reports?

TIP automatically stores log in, screened baggage, and screener TIP performance information. The report is generated directly from log in and performance data collected automatically and stored in the TIP system.

Note: TIP has built-in safeguards so that these data cannot be changed or deleted.

Screener Log Report: Overview and Generation
--

What is a Screener Log Report?

A Screener Log Report is a summary of which screeners worked each day, their locations, and the times they logged in. It includes the dates they worked, their names, ID numbers, security company, location, and log in and log out times (see Figure 2).

What does each column heading mean?

1. **Date:** The date the screener logged in
2. **Name:** The name of the screener who logged in
3. **ID #:** The log in ID number of the screener who logged in
4. **Company:** The screener's security company
5. **Location:** Where the screener logged in
6. **Log In Time:** The time the screener logged in
7. **Log Out Time:** The time the screener logged out

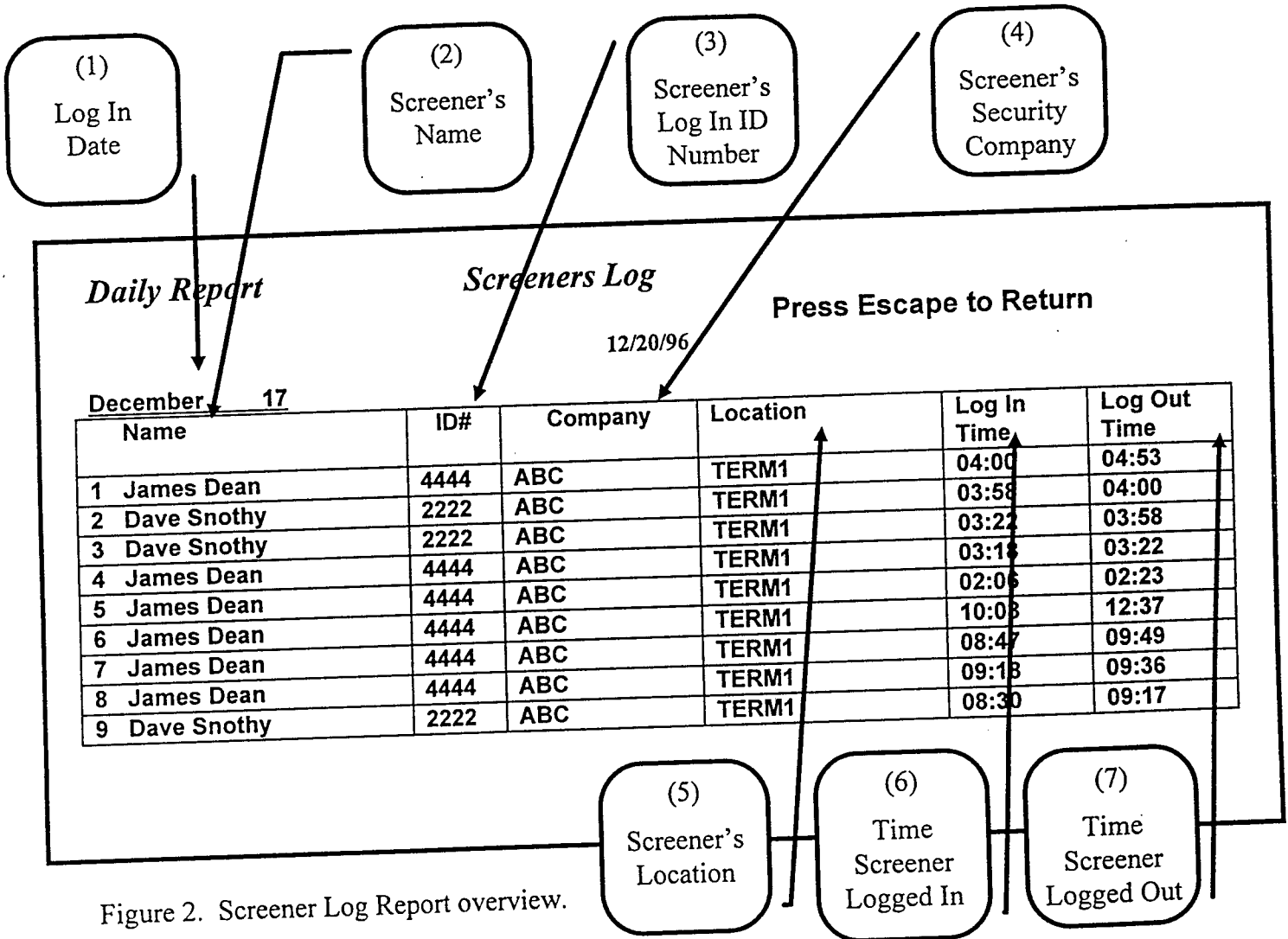


Figure 2. Screener Log Report overview.

How do I view a Screener Log Report?

(See Figures 3a and 3b)

Step 1. Click on View Reports from the menu bar.

Step 2. Click on **Screener Log**.

Step 3. Click on the desired month/year.

Step 4. Click on the View button.

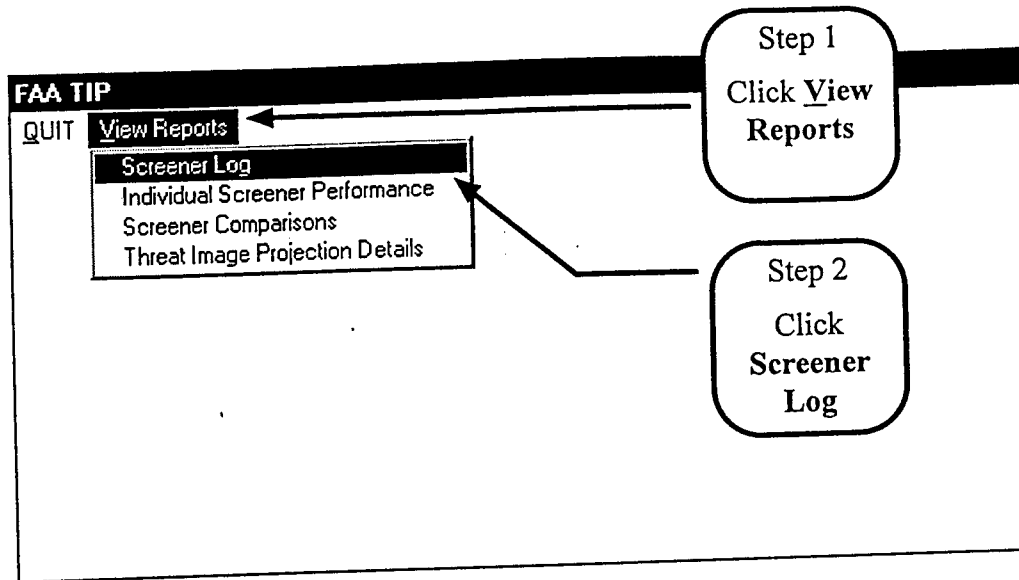


Figure 3a. Viewing a Screener Log Report - steps 1 and 2.

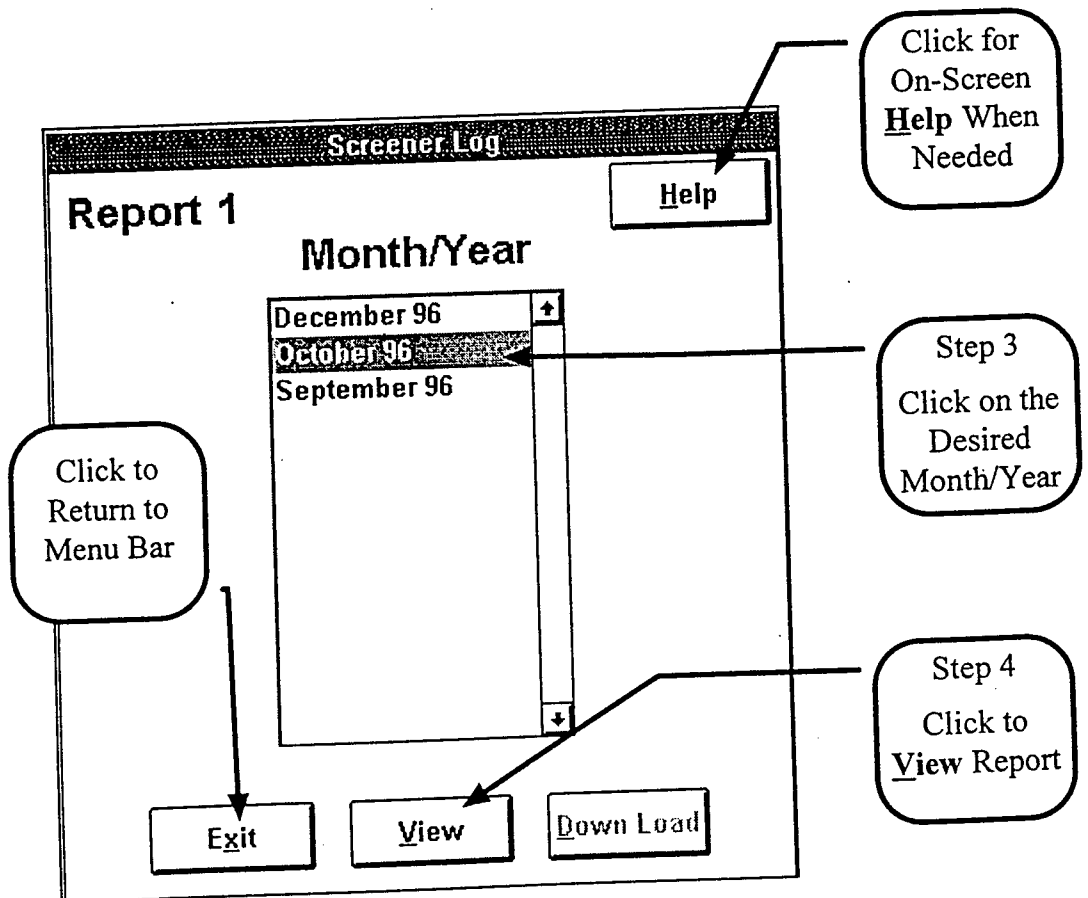


Figure 3b. Viewing a Screener Log Report - steps 3 and 4.

Individual Screener Performance Summary Comparisons Report: Overview and Generation

What is an Individual Screener Performance Summary Comparisons Report?

An Individual Screener Performance Summary Comparisons Report presents an individual screener's daily performance for a given month (see Figure 4).

What does each column heading mean?

- | | |
|--|---|
| 1. Screener's name, ID #, and location | |
| 2. Date: | The date the screener logged in |
| 3. # of bags screened: | Number of bags that individual screened that day |
| 4. TIPs Presented: | Number of TIPs presented |
| 5. N_H : | Number of correctly identified TIPs (hits) |
| 6. N_{FA} : | Number of bags incorrectly identified as threats (false alarms) |
| 7. N_M : | Number of TIPs not identified (misses) |
| 8. P_d : | Proportion of TIPs correctly identified (hits) |
| 9. P_{FA} : | Proportion of bags incorrectly identified as threats (false alarms) |
| 10. d' : | Technical measure of performance |
| 11. RTN_H : | Average time for correct identification of a TIP (hit) |
| 12. RTN_{FA} : | Average time for incorrect identification (false alarm) |

Individual Screener Performance Summary Comparisons Report: Overview and Generation

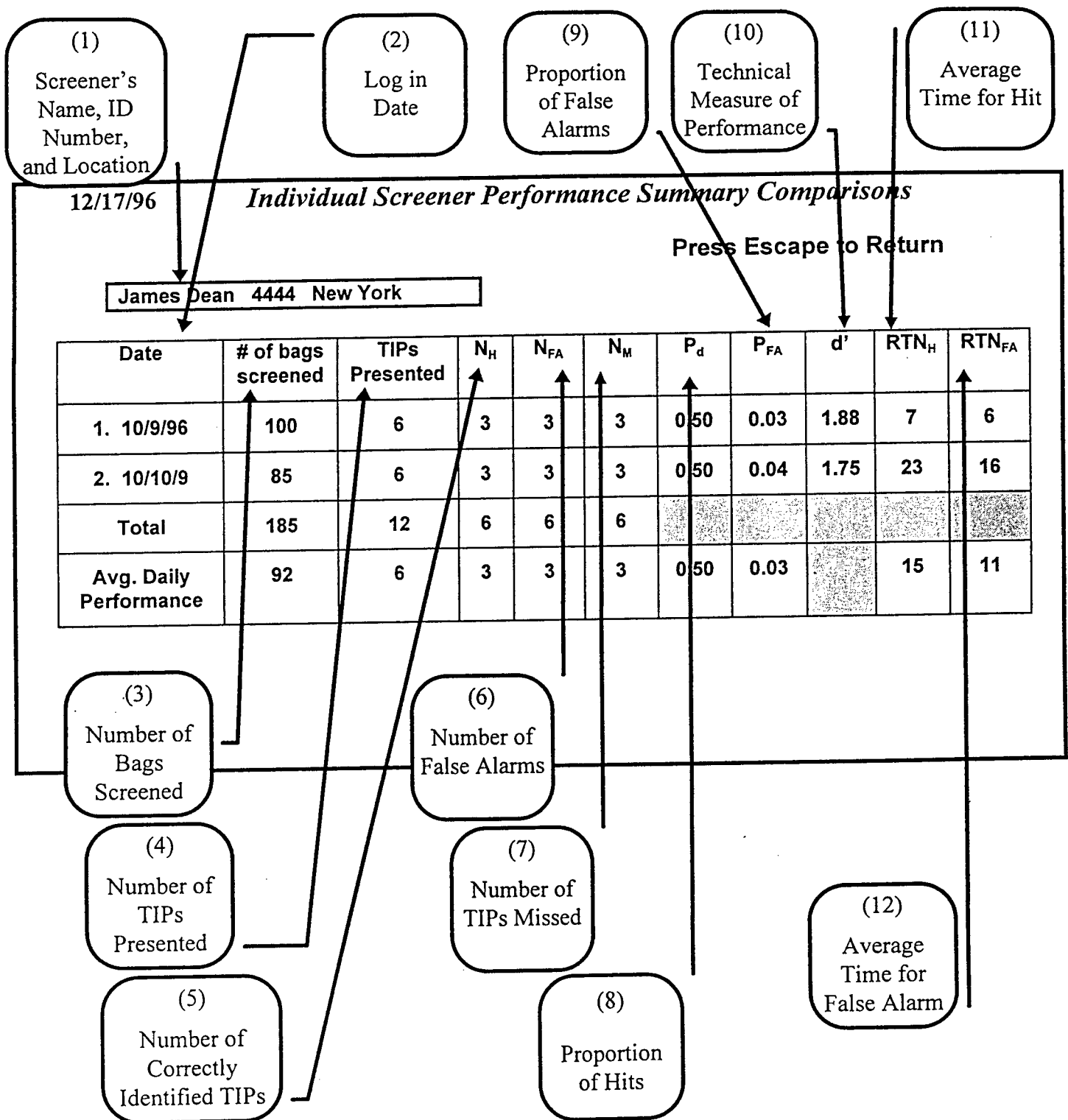


Figure 4. Individual Screener Performance Summary Comparisons Report overview.

How do I view an Individual Screener Performance Summary Comparisons Report?

(See Figures 5a and 5b)

- Step 1. Click on View Reports from the menu bar.

Step 2. Click on **Individual Screener Performance**.

Step 3. Click on the desired screener name/ID number.

Step 4. Click on the desired month/year.

Step 5. Click on the View button.

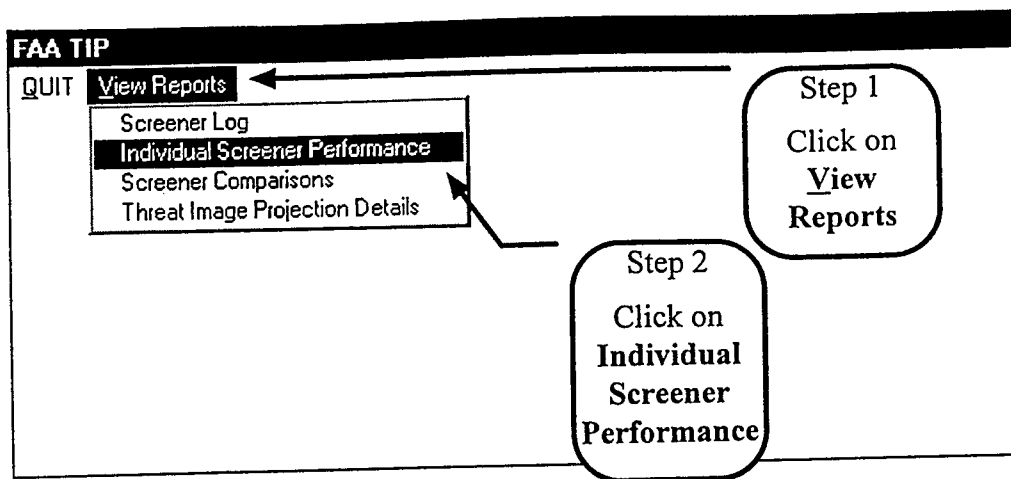


Figure 5a. Viewing an Individual Screener Performance Summary Comparisons Report - steps 1 and 2.

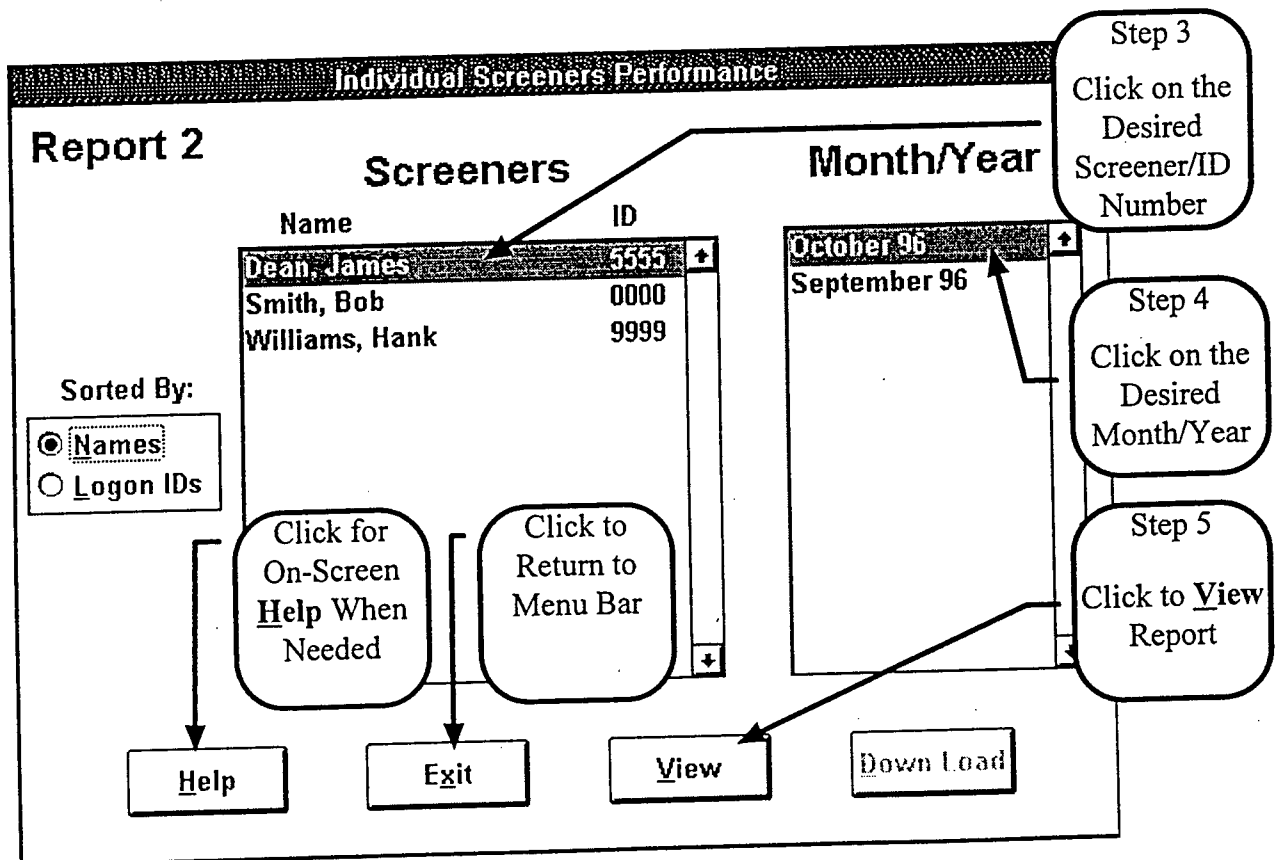


Figure 5b. Viewing an Individual Screener Performance Summary Comparisons Report - steps 3, 4, and 5.

Screener Comparisons Report: Overview and Generation

What is a Screener Comparisons Report?

A Screener Comparisons Report displays the performance of multiple screeners for a given month (see Figure 6).

What does each column heading mean?

- | | |
|---------------------|--|
| 1. Date: | Month and year of the report |
| 2. Name/ID#: | Screener's name and ID number |
| 3. # shifts worked: | Number of shifts worked by screener |
| 4. # bags screened: | Number of bags screened |
| 5. TIPs Presented: | Number of TIPs presented |
| 6. N_H : | Number of correctly identified TIPs (hits) |
| 7. N_{FA} : | Number of bags incorrectly identified as threats (false alarms) |
| 8. N_M : | Number of TIPs not identified (misses) |
| 9. P_d : | Proportion of correctly identified TIPs (hits) |
| 10. P_{FA} : | Proportion of bags incorrectly identified as threats (false alarms) |
| 11. d' : | Technical measure of performance |
| 12. RTN_H : | Average time in seconds for correct identification of a TIP (hit) |
| 13. RTN_{FA} : | Average time in seconds for bags incorrectly identified as threats (false alarm) |

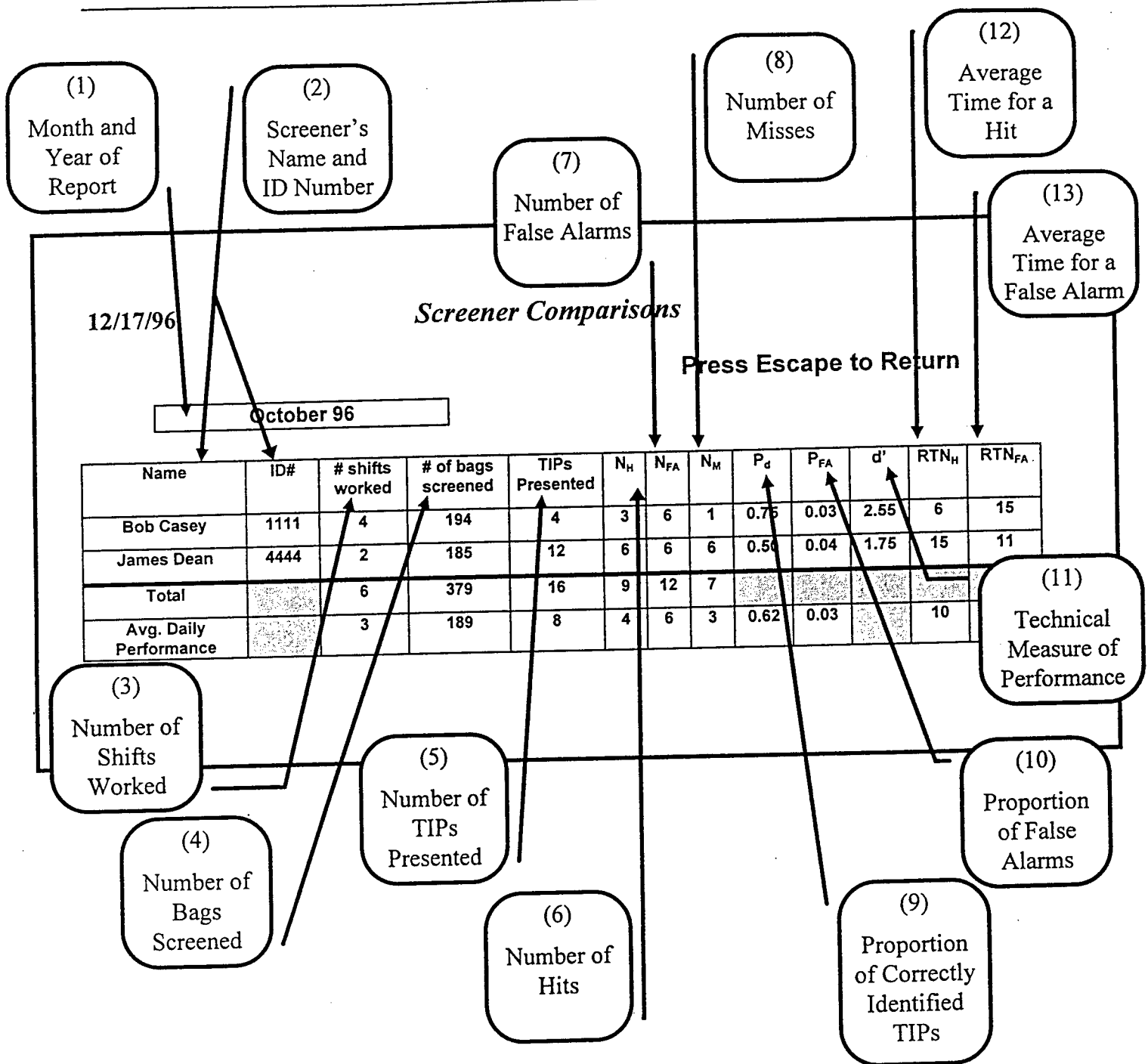


Figure 6. Screener Comparisons Report overview.

How do I get a Screener Comparisons Report?

(See Figures 7a and 7b)

Step 1. Click on View Reports from the menu bar.

Step 2. Click on **Screener Comparisons**.

Step 3. Click on the desired month/year.

Step 4. Click on the View button.

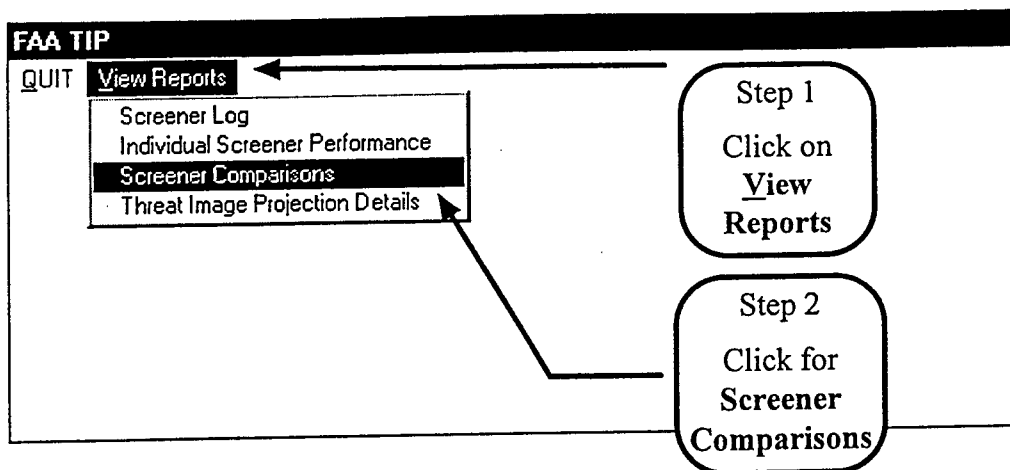


Figure 7a. Viewing a Screener Comparisons Report - steps 1 and 2.

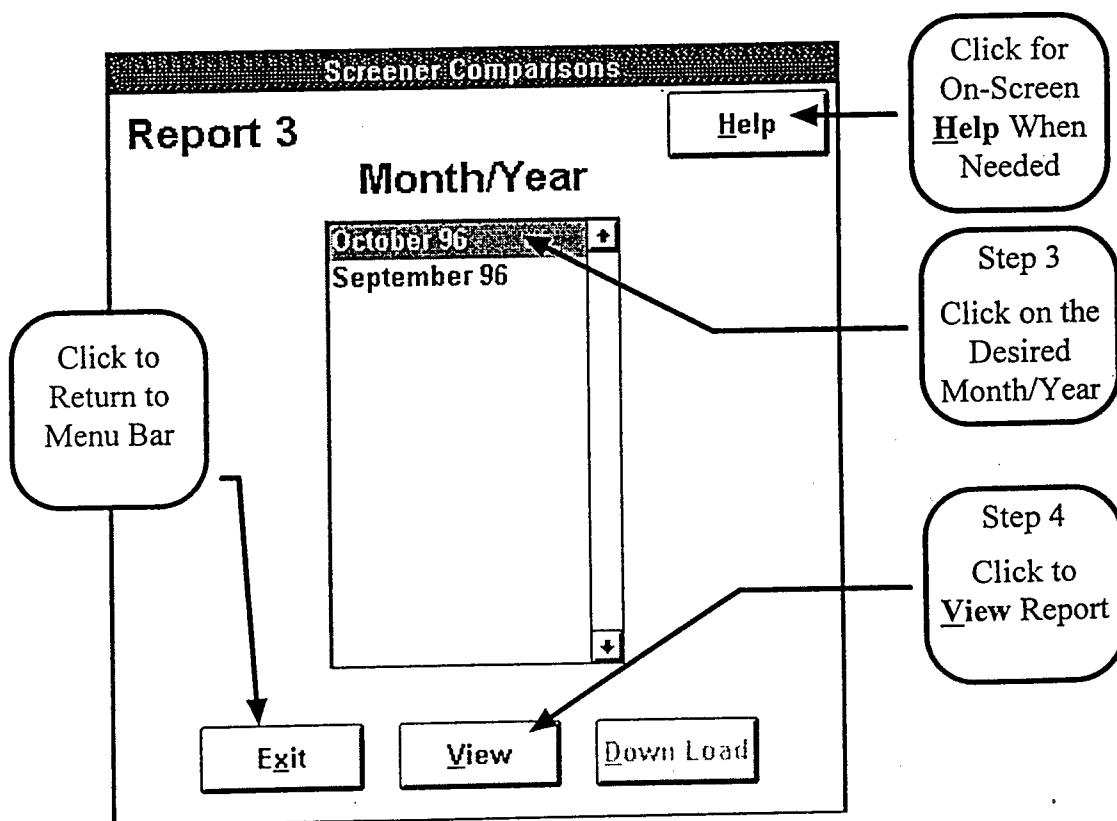


Figure 7b. Viewing a Screener Comparisons Report - steps 3 and 4.

Threat Image Projection Details Report: Overview and Generation

What is a Threat Image Projection Details Report?

The Threat Image Projection Details Report provides detailed information about every TIP image presented during the baggage X-ray process including the screeners' decision outcomes (detect, miss, false alarm) and the TIP threat category (e.g., bomb) (see Figure 8).

What does each column heading mean?

1. **Date/Image Time:** Date and time image was presented
2. **Name/ID#:** Name and ID number of screener
3. **Threat Name:** Assigned code identifying the specific threat
4. **Category/
SubCategory:** Threat category and threat subcategory
5. **Decision Outcome:**
 - Hit:** TIP correctly identified by the screener
 - Miss:** TIP presented but not detected by the screener
 - False Alarm:** A bag incorrectly identified as a threat by the screener
6. **Hit Resp Time:** Time to correctly identify a TIP
7. **False Resp Time:** Time to incorrectly identify a bag as a threat

Threat Image Projection Details Report: Overview and Generation

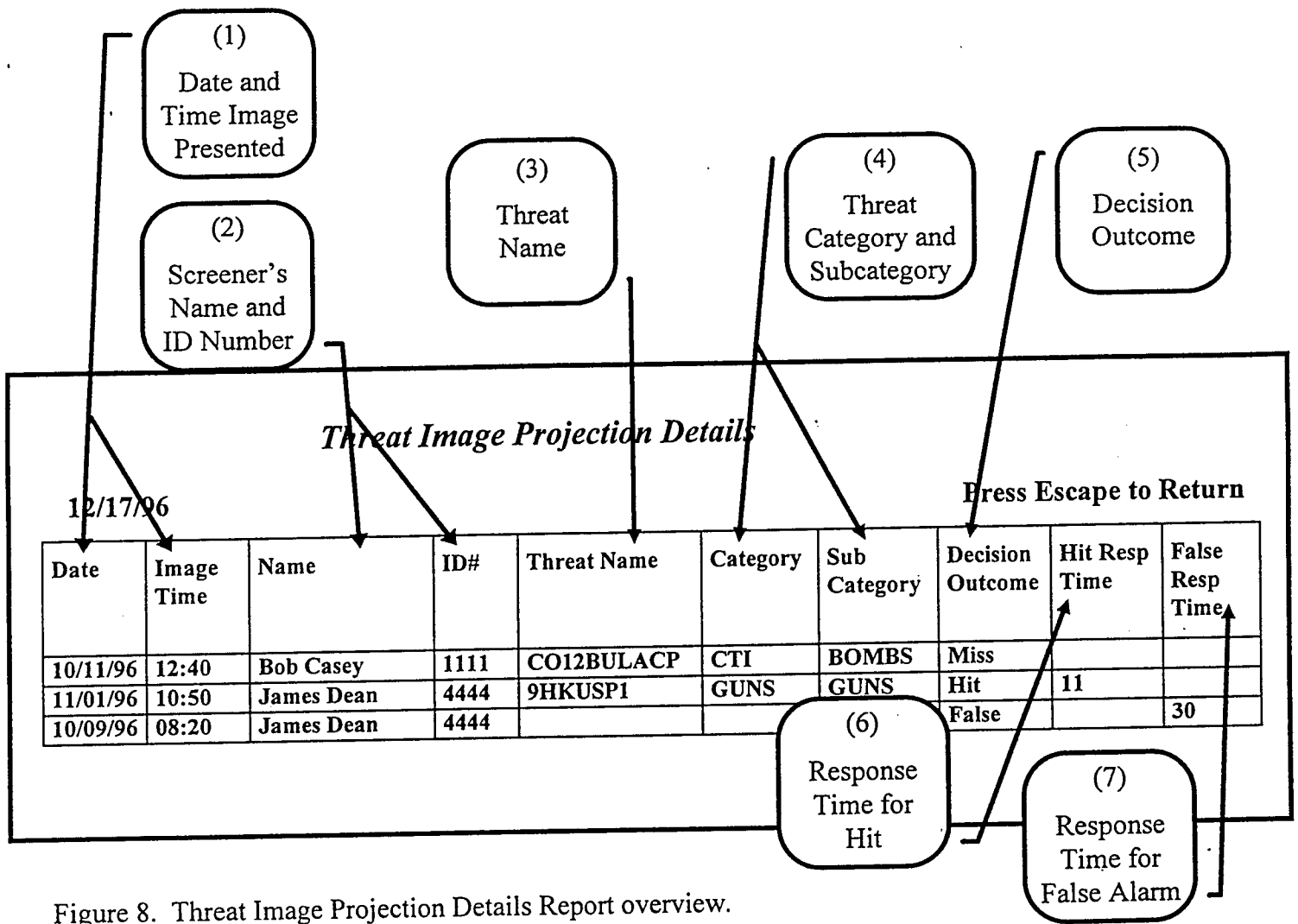


Figure 8. Threat Image Projection Details Report overview.

How do I get a Threat Image Projection Details Report?

(See Figure 9a and 9b)

Step 1. Click on View Reports from the menu bar.

Step 2. Click on **Threat Image Projection Details**.

Step 3. Click on the desired month/year.

Step 4. Click on the View button.

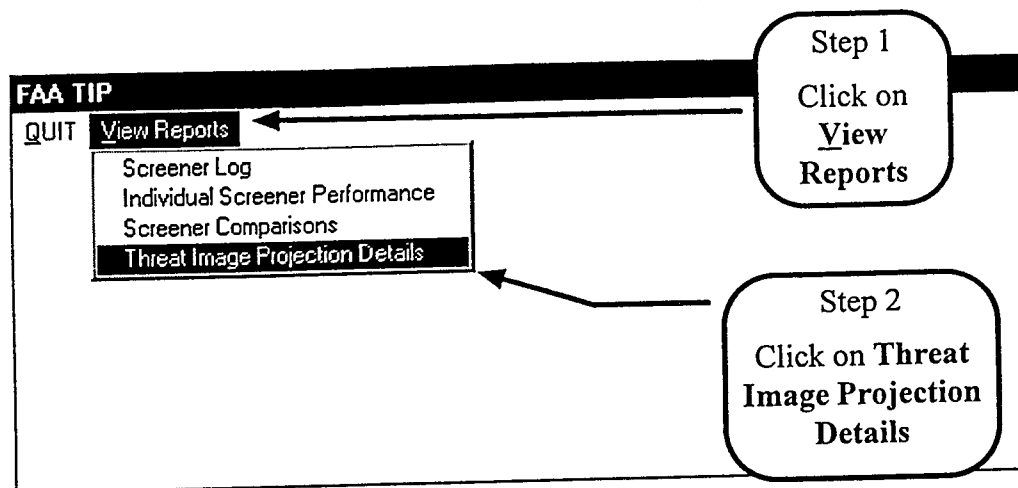


Figure 9a. Viewing a Threat Image Projection Details Report - steps 1 and 2.

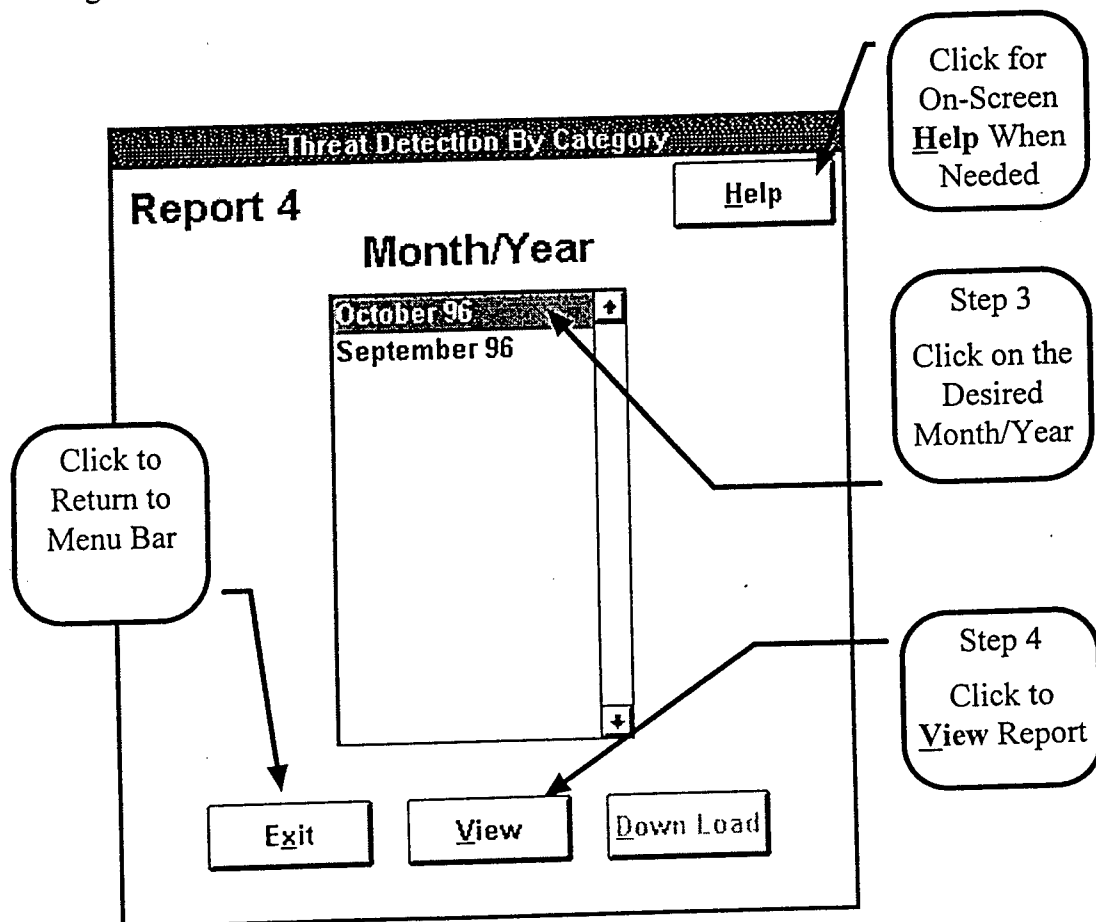


Figure 9b. Viewing a Threat Image Projection Details Report - steps 3 and 4.

Log Out

Log Out

How do I log out?

(See Figure 10)

Step 1. Step 1. Click on Quit from the menu bar.

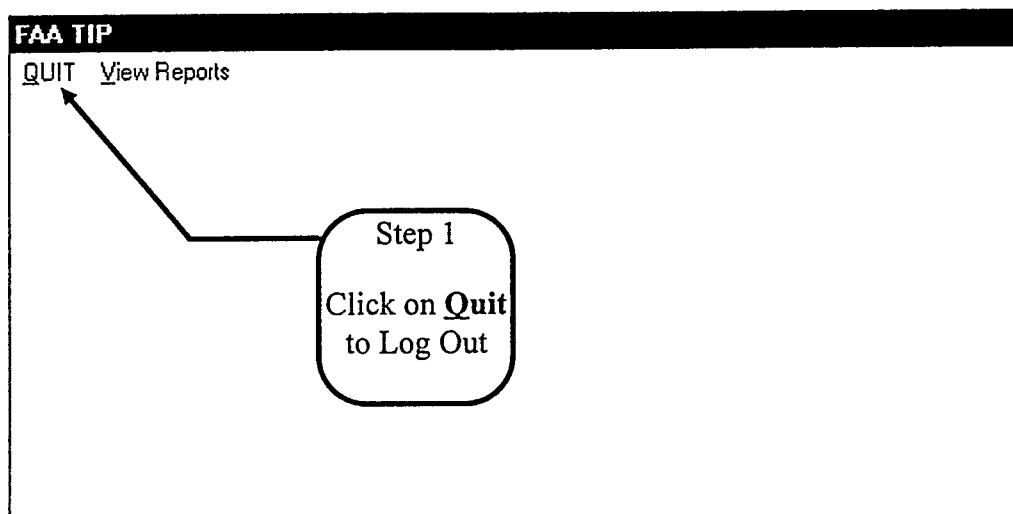


Figure 10. Log out procedure.

Note: After you have successfully logged out, the log in window will be displayed.